

Algebraic Aspects of Linear Differential and Difference Equations

Peter A. Hendriks
University of Groningen
Department of Mathematics
P.O. Box 800
9700 AV Groningen
The Netherlands
e-mail p.a.hendriks@math.rug.nl

VISIT...

LANZAROTE
Caliente.COM

Rijksuniversiteit Groningen

Algebraic Aspects of Linear Differential
and Difference Equations

Proefschrift

ter verkrijging van het doctoraat in de
Wiskunde en Natuurwetenschappen
aan de Rijksuniversiteit Groningen
op gezag van de
Rector Magnificus Dr. F. van der Woude,
in het openbaar te verdedigen op
vrijdag 29 november 1996
des namiddags te 4.15 uur

door

Peter Anne Hendriks

geboren op 9 september 1968
te Groningen

Promotor: Prof.dr. M. van der Put
Referent: Dr. F. Beukers

Aan mijn ouders

Contents

1	Introduction	3
2	Galois Action on Solutions of a Differential Equation	7
2.1	Introduction	7
2.2	The universal field of $k((x))$	8
2.3	The k -structure on the space of solutions	12
2.3.1	Remarks	13
2.4	Rational solutions of Riccati	13
2.5	Algebraic solutions of the Riccati equation and examples	14
2.5.1	Equations of order two	16
2.5.2	Equations of order three	17
2.5.3	Remarks	19
2.6	Symmetries	19
2.6.1	Symmetries of L	20
2.6.2	Transforming algebraic solutions of Riccati	22
2.6.3	Forms of a differential operator	22
2.6.4	Construction of special differential equations	24
2.6.5	Examples	24
3	Shidlovskii irreducibility	29
3.1	Introduction	29
3.2	Preliminaries	30
3.3	Siegel normality	34
3.4	Shidlovskii irreducibility	37
3.5	Examples	43
4	An algorithm determining the difference Galois group of second order linear difference equations	49
4.1	Introduction	49
4.2	Preliminaries on difference Galois theory	50
4.3	First order difference equations	52
4.4	Second order difference equations	53
4.4.1	The Riccati equation	53

4.4.2	G is reducible	58
4.4.3	G is imprimitive	60
4.4.4	G contains $Sl(2, \mathbf{Q})$	62
4.5	Examples	63
4.5.1	Sequences spaces	63
4.5.2	The case where an extension of the constant field is needed	70
5	An algorithm for computing a standard form for second order linear q-difference equations	71
5.1	Introduction	71
5.2	A short introduction to algebraic aspects of q -difference equations.	71
5.3	First order q -difference equations	75
5.4	Second order q -difference equations	76
5.4.1	The Riccati equation	76
5.4.2	G is reducible	81
5.4.3	G is imprimitive	83
5.4.4	G contains $Sl(2, \mathbf{C})$	84
5.5	Examples	85
5.5.1	Sequences spaces	85
5.5.2	Hypergeometric q -difference equations	87
6	On the classification of a class of q-difference equations	91
6.1	Introduction	91
6.2	Picard–Vessiot Theory	91
6.3	Classification of q -Difference Modules	92
6.4	Tannakian Categories and the q -Difference Galois Group	97

Chapter 1

Introduction

This thesis is about some algebraic and algorithmic aspects of linear differential, difference and q -difference equations over the field of rational functions $\mathbf{C}(z)$.

The starting-point for a great part of this thesis was Kovacic's algorithm [Kov86]. Kovacic's algorithm computes a Liouvillian solution of the second order linear differential equation $y'' + ay' + by = 0$, where $a, b \in \mathbf{C}(z)$, provided a Liouvillian solution exists. We will define the notion Liouvillian solution. A differential field extension $L \supseteq \mathbf{C}(z)$ is called a Liouvillian extension if there is a finite sequence of differential fields

$$\mathbf{C}(z) = L_0 \subset L_1 \subset \cdots \subset L_{n-1} \subset L_n = L$$

such that $L_i = L_{i-1}(a_i)$, where one of the following three cases holds:

1. a_i is algebraic over L_{i-1}
2. a_i satisfies a differential equation $y' = by$, where $b \in L_{i-1}$
3. a_i satisfies a differential equation $y' = b$, where $b \in L_{i-1}$

A solution f of a linear differential equation is called Liouvillian if f lies in some Liouvillian extension.

Kovacic's algorithm is based on the results of differential Galois theory. For a short introduction of differential Galois theory we refer to the sections 2.1 and 3.2 in this thesis. Many interesting properties of linear differential equations can be characterized in terms of the differential Galois group and its action on the vector space of solutions.

For instance a linear differential equation is irreducible (that is the corresponding differential operator does not factor over $\mathbf{C}(z)$) if and only if the differential Galois group G associated to this equation acts irreducibly on the vector space of solutions. All solutions of a linear differential equation are algebraic if and only if the differential Galois group G is finite. And all the solutions of a linear

differential equation are Liouvillian if and only if the identity component G^0 of the differential Galois group G is solvable.

Two other interesting properties of linear differential equations are being Siegel normal and being Shidlovskii irreducible. These properties play a role in some part of transcendental number theory. In chapter 3 these properties will be characterized in terms of the standard representation of the differential Galois group G . Further there will be explained how these characterizations can be used to verify Siegel normality or Shidlovskii irreducibility in some concrete practical examples. Chapter 3 is published before [Hen94].

Back to Kovacic's algorithm. For any solution $y \neq 0$ of the differential equation $y'' + ay' + by = 0$ the element $u = \frac{y'}{y}$ satisfies the associated Riccati equation $u' + u^2 + au + b = 0$. The differential equation $y'' + ay' + by = 0$ has a Liouvillian solution if and only if the associated Riccati equation $u' + u^2 + au + b = 0$ has an algebraic solution. The proof of this statement is based on differential Galois theory and the classification of the algebraic subgroups of $Sl(2, \mathbf{C})$. Kovacic's algorithm tries to compute a solution of the Riccati equation that is algebraic and of minimal degree n over $\mathbf{C}(z)$. It is shown in [Kov86] that this minimal degree can be 1, 2, 4, 6 or 12. For analogous results for third order linear differential equations we refer to [SU93].

Suppose now that $a, b \in \mathbf{Q}(z)$. In general the algorithm described in [Kov86] generates algebraic numbers in a rather chaotic way. Therefore in some practical cases the algorithm did not work very well. The coefficients of the monic irreducible polynomial of a solution of the Riccati equation that is algebraic and of minimal degree over $\mathbf{C}(z)$ are in $C(z)$ where C is a finite algebraic extension of $\mathbf{Q}$. In chapter 2 bounds are given for the degree of the extension $C \supset \mathbf{Q}$. Analogous results are obtained for third order differential equations. These bounds help to make Kovacic's algorithm more efficient. Chapter 2 is published before [HP95].

Recently Galois theory of difference equations is developed by M. van der Put and M.F. Singer [PS96]. In chapters 4 and 5 algorithms are presented for determining the difference Galois group and the q -difference Galois group of second order difference and q -difference equations respectively. These algorithms can be considered as the analogue for difference and q -difference equations of Kovacic's algorithm for differential equations. Further the notion of Liouvillian solutions is introduced for difference and q -difference equations. If the difference or q -difference Galois group is not too big (i.e does not contain the group $Sl(2, \mathbf{C})$) then it is possible to compute two linearly independent solutions in a certain sequences space.

In some respects difference and q -difference equations are more difficult to treat than differential equations, due to the fact that the Picard–Vessiot rings associated to difference or q -difference equations are in general not integral domains but only reduced algebras. But on the other hand the finite primitive groups that cause the most troubles in the differential case do not occur as differ-

ence or q -difference Galois group. Chapter 4 is accepted for publication [Hen96].

In chapter 6 q -difference equations over the field $\mathbf{C}(z)$ are classified, where q is an m th root of unity. In this case there is not a unique Picard–Vessiot ring for every system of q -difference equations. Therefore it is not possible to define the q -difference Galois group in the usual way. If q is a root of unity then we will use the theory of Tannakian categories for a suitable definition of the q -difference Galois group.

Chapter 2

Galois Action on Solutions of a Differential Equation

2.1 Introduction

Consider a second order differential equation of the form $y'' + ay' + by = 0$ with $a, b \in \mathbf{Q}(x)$. If one works over the algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$ then differential Galois theory is available. This theory tells us that there exists a Picard–Vessiot field $F \supset \overline{\mathbf{Q}}(x)$ satisfying

1. $F \supset \overline{\mathbf{Q}}(x)$ is an extension of differential fields.
2. The field of constants of F is $\overline{\mathbf{Q}}$.
3. The equation has two $\overline{\mathbf{Q}}$ -linear independent solutions in F .
4. F is minimal with respect to the conditions (2) and (3).

The theory continues as follows:

1. F is unique up to d-isomorphism.
2. Let G be the group of d-isomorphism of F over $\overline{\mathbf{Q}}(x)$. Then the set of G -invariant elements of F is $\overline{\mathbf{Q}}(x)$.
3. Let $V \subset F$ be the set of solutions of the differential equation. Then V is a two-dimensional vector space over $\overline{\mathbf{Q}}$. The group G acts faithfully on V and the image of G in $\text{Aut}(V)$ is a linear algebraic subgroup.

A solution of the Riccati equation is an $u \in F$ of the form $\frac{v'}{v}$ with $v \in V$ and $v \neq 0$. Kovacic's algorithm tries to compute the solutions of the Riccati equation. The first part of this algorithm tries to find solutions $u = \frac{v'}{v} \in \overline{\mathbf{Q}}(x)$. This means that $\overline{\mathbf{Q}}v$ is a G -invariant line in V .

The origin of this paper is the question to find out for which field $C \supset \mathbf{Q}$ the solution u lies in $C(x)$.

Suppose that the group G has the following form: V has a basis v_1, v_2 such that G consists of all $g \in \text{Aut}(V)$ with $g(v_1) = cv_1$ and $g(v_2) = c^{-1}v_2$ with $c \in \overline{\mathbf{Q}}^*$. Then V has only two G -invariant lines and $u_i = \frac{v'_i}{v_i}$, $i = 1, 2$, are the only solutions of the Riccati which lie in $\overline{\mathbf{Q}}(x)$.

The intuitive reasoning is now the following: A Galois automorphism of $\overline{\mathbf{Q}}$ can at most permute $\{u_1, u_2\}$. Hence u_1, u_2 lie in $C(x)$ where $[C : \mathbf{Q}] \leq 2$. An explicit example of this situation is the equation $y'' = 2x^{-4}y$. The field C is here $\mathbf{Q}(\sqrt{2})$.

In the next two sections we will develop the theory justifying this intuitive idea. We note that there is no suitable differential Galois theory which works over a constant field of characteristic 0 which is not algebraically closed. The next sections provides some theory in a special case. In later sections we will summarize and correct the results of [HP93] and we will give some more applications. Further a theory of symmetries and forms of a differential operator is developed in order to construct differential operators with special features with respect to the field of constants which is needed for the Riccati equation.

We would like to thank M. F. Singer and F. Ulmer for pointing out a mistake in [HP93]. Unfortunately, it was too late to correct the paper before publication.

2.2 The universal field of $k((x))$

Let k be a field of characteristic 0 with algebraic closure $\bar{k}$. One considers differential equations over the differential field $K = k((x))$ with the differentiation $' = x \frac{d}{dx}$ given by $(\sum a_n x^n)' = \sum n a_n x^{n-1}$. We want to make a *universal field extension* $\Omega \supset K$ for which every differential equation over K has a full set of solutions. More precisely one defines Ω as follows:

1. $\Omega \supset K$ is an extension of d-fields.
2. The field of constants of Ω is $\bar{k}$.
3. For every (homogeneous linear) differential equation

$$y^{(d)} + a_1 y^{(d-1)} + \dots + a_{d-1} y^{(1)} + a_0 y = 0$$

with coefficients in a finite extension of K the space of solutions in Ω is a vector space over $\bar{k}$ of dimension d .

4. Ω is minimal with respect to the conditions (2) and (3).

As is well known condition (3) is equivalent to (3*) Every matrix differential equation $v' = Av$, where the matrix A has coefficients in a finite extension K has a fundamental matrix with coefficients in Ω .

Theorem 2.2.1 *Ω with the above properties exists and is unique up to isomorphism.*

Proof. The field Ω must certainly contain the following things:

1. $\bar{k}$.
2. For every $m \geq 1$ an element $x^{\frac{1}{m}}$.
3. A solution of $y' = 1$, since Ω has two linearly independent solutions of $y'' = 0$.
4. A non zero solution of $y' = qy$ for every $q \in \cup_{m \geq 1} x^{-1/m} \bar{k}[x^{-1/m}]$.

One would like to see the solutions of the equations above as certain functions. This is however *a priori* not possible, since we would have to explain then what the product of a formal Laurent series with a solution of say $y' = 1$ means. Therefore we will build up Ω in a very algebraic way.

Let $\mathcal{Q}$ denote the additive group (or $\bar{k}$ -vector space) $\cup_{m \geq 1} \bar{k}[x^{-1/m}]$. Further, $\bar{K}$ denotes the algebraic closure of K . We note that $\bar{K}$ is generated over K by $\bar{k}$ and the elements $x^{\frac{1}{m}}$, $m \geq 1$. We remark that, in general, $\bar{k}((x))$ is not algebraic over K , but every element of $\bar{K}$ can be represented by a Laurent series in $\bar{k}((x^{\frac{1}{m}}))$ for some $m \geq 1$. We start with a polynomial ring in many variables $R_0 := \bar{K}[L, E(q)]_{q \in \mathcal{Q}}$ and we define a differentiation on R_0 by:

1. For $f = \sum_{\lambda \in \mathbf{Q}} c_{\lambda} x^{\lambda} \in \bar{K}$ one has $f' = \sum_{\lambda \in \mathbf{Q}} \lambda c_{\lambda} x^{\lambda} \in \bar{K}$. This is the unique extension of the differentiation $' = x \frac{d}{dx}$ to $\bar{K}$.
2. $L' = 1$.
3. $E(q)' = qE(q)$.

It is easily verified that the above defines a unique differentiation on R_0 . Let $I \subset R_0$ denote the ideal generated by $E(q_1 + q_2) - E(q_1)E(q_2)$ (all $q_1, q_2 \in \mathcal{Q}$) and $E(\lambda) - x^{\lambda}$ (all $\lambda \in \mathbf{Q}$). The ideal I is invariant under differentiation. Indeed,

$$(E(q_1 + q_2) - E(q_1)E(q_2))' = (q_1 + q_2)(E(q_1 + q_2) - E(q_1)E(q_2)), \text{ and}$$

$$(E(\lambda) - x^\lambda)' = \lambda(E(\lambda) - x^\lambda)$$

Let $R := R_0/I$ and let l and $e(q)$ denote the images of L and $E(q)$ in R . Since the ideal I is invariant under differentiation one finds a differentiation on R and one has the following properties:

1. $l' = 1$.
2. $e(q)' = qe(q)$ for all $q \in \mathcal{Q}$.
3. $e(q_1 + q_2) = e(q_1)e(q_2)$ for all $q_1, q_2 \in \mathcal{Q}$.
4. $e(\lambda) = x^\lambda$ for all $\lambda \in \mathbf{Q}$.

□

Lemma 2.2.2 *The ring R has no zero divisors and there is no prime ideal ($\neq 0, R$) in R which is invariant under differentiation.*

Proof. Choose $q_1, \dots, q_s \in \mathcal{Q}$ such that $1, q_1, \dots, q_s$ are linearly independent over $\mathbf{Q}$. Consider the subring

$$A := \bar{K}[l, e(q_1), e(-q_1), \dots, e(q_s), e(-q_s)] \text{ of } R$$

Every finite subset of R lies in such a subring of A . One can see that there are only the trivial relations $e(q_1)e(-q_1) = 1, \dots, e(q_s)e(-q_s) = 1$ among the generators of A over $\bar{K}$. That means that A is isomorphic to the ring $\bar{K}[X, T_1, T_1^{-1}, \dots, T_s, T_s^{-1}]$. This ring is a localization of the polynomial ring $\bar{K}[X, T_1, \dots, T_s]$. In particular, A and R have no zero divisors. It is easily seen that A can have no non-trivial ideal that is invariant under differentiation. This implies the same statement for R . □

Lemma 2.2.3 *Let Ω denote the field of fractions of R , then Ω is a d -field containing $\bar{K}$ and the field of constants of Ω is $\bar{k}$.*

Proof. Let $u \in \Omega$ satisfy $u' = 0$ and $u \neq 0$. For suitable $q_1, \dots, q_s \in \mathcal{Q}$ such that $1, q_1, \dots, q_s$ are linearly independent over $\mathbf{Q}$ one can write $u = \frac{f}{g}$ where $f, g \in A := \bar{K}[l, e(q_1), \dots, e(q_s)]$. The generators of A over $\bar{K}$ have no relations and so A is an ordinary “free” polynomial ring over $\bar{K}$ in $s + 1$ generators. One may assume that $\text{g.c.d.}(f, g) = 1$. Now $u' = 0$ implies that $f'g = fg'$ and in particular f divides f' and g divides g' .

Write f as a finite sum $\sum_{q \in \mathbf{N}q_1 + \dots + \mathbf{N}q_s} a_q e(q)$ with each $a_q \in \bar{K}[l]$ and where $\mathbf{N}$ denotes the set of non-negative integers. Then $f' = \sum (a'_q + qa_q)e(q)$ has a total degree which is less or equal to the total degree of f . Hence $f' = Bf$ for some $B \in \bar{K}$ and also $g' = Bg$. For each q one finds the relation $a'_q + qa_q = Ba_q$. We will need the following result.

Lemma 2.2.4 *If the equation $a' + ha = 0$ with $h \in \bar{K}$ has a non-zero solution in $\bar{K}[l]$, then $h \in \mathbf{Q} + \cup_{n \geq 1} x^{1/n} \bar{k}[[x^{1/n}]]$.*

Proof. Write $a = a_0 + a_1 l + \dots + a_d l^d$ with all $a_i \in \bar{K}$ and with $a_d \neq 0$. Using $l' = 1$ and looking at the coefficient of l^d , one finds $a'_d + ha_d = 0$. Write $a_d = cx^\lambda(1 + \sum_{\mu > 0} c_\mu x^\mu)$ with $c \in \bar{k}$, $c \neq 0$ and $\lambda \in \mathbf{Q}$. Then it is clear that h has the form specified in the lemma. $\square$

We continue the proof of Lemma 2.2.3. If $a_q \neq 0$ then B must have the form $B = q + h$ where $h \in \mathbf{Q} + \cup_{n \geq 1} x^{1/n} \bar{k}[[x^{1/n}]]$. This can happen for only one q since $1, q_1, \dots, q_s$ are supposed to be linearly independent over $\mathbf{Q}$. Hence $f = a_q e(q)$ and similarly $g = b_r e(r)$ for some $r \in \mathbf{N}q_1 + \dots + \mathbf{N}q_s$. However $q - r \in \mathbf{Q} + \cup_{n \geq 1} x^{1/n} \bar{k}[[x^{1/n}]]$ implies that $q = r$. Since $\text{g.c.d.}(f, g) = 1$ it follows that $q = r = 0$ and $f, g \in \bar{K}[l]$ and $B \in \mathbf{Q} + \cup_{n \geq 1} x^{1/n} \bar{k}[[x^{1/n}]]$. We may assume that g is monic as polynomial in l . Then g divides g' implies that $g = 1$ since the degree of g' is less than the degree of g . Hence $u = f \in \bar{K}[l]$ and $f' = 0$. Write $f = f_0 + f_1 l + \dots + f_d l^d$ with $f_0, \dots, f_d \in \bar{K}$ and $f_d \neq 0$. Looking at the coefficient of l^d in $f' = 0$ one finds that $f_d = c \in \bar{k}$ and $c \neq 0$. If $d \geq 1$ then the coefficient of l^{d-1} gives the equation $f'_{d-1} = -dc$. It is easily seen that no element in $\bar{K}$ satisfies this relation. Hence $d = 0$ and $u \in \bar{k}$. This finishes the proof of Lemma 2.2.3. $\square$

Lemma 2.2.5 *Every differential equation over a finite extension of K has a basis of solutions in Ω .*

Proof. We will use here the language of differential modules over K . Such a module (M, δ) is a finite dimensional vector space M over K with an operator δ on it, satisfying: δ is additive and $\delta(km) = k'm + k\delta(m)$ for $k \in K$ and $m \in M$. It is well known how to translate a homogeneous linear differential equation (or a differential equation in matrix form) into a differential module. In the following we will replace K by finite extensions of K without changing the notation. We use now the formal classification of differential equations (cf. [Lev75]). After a finite field extension of K , the differential module M is a direct sum of submodules N . For each N there is a $q \in \mathbf{Q}$ such that the operator $\delta - q$ is nilpotent. Then one easily sees that the field $\bar{K}(l, e(q)) \subset \Omega$ contains d linearly independent solutions of N , where d denotes the dimension of N . Hence Ω has the desired property. $\square$

Lemma 2.2.6 *The field Ω is the universal extension of K .*

Proof. The minimality of Ω has already been discussed. The other properties are contained in Lemmas 2.2.3 and 2.2.5.

Thus we have shown the existence of a universal field. Let Ω' be another universal field. Then there is a differential homomorphism $\sigma : R \rightarrow \Omega'$. According to lemma 2.2.2, the kernel of σ is 0 and σ extends to a differential homomorphism σ of Ω to Ω' . The minimality of Ω' implies that σ is an isomorphism. $\square$

Corollary 2.2.7 *Let G^+ be the group of all automorphisms σ of the field Ω such that σ is the identity on K and σ commutes with the differentiation on Ω . Let G denote the normal subgroup of G^+ consisting of the σ which are the identity on $\bar{k}$. Then the following sequence is split exact.*

$$0 \rightarrow G \rightarrow G^+ \rightarrow \text{Gal}(\bar{k}/k) \rightarrow 0$$

Proof. Let $\tau \in \text{Gal}(\bar{k}/k)$. Extend τ first to an automorphism τ' of $\bar{K}$ by $\tau'(\sum_{\lambda \in \mathbf{Q}} a_\lambda x^\lambda) = \sum_{\lambda} (\tau a_\lambda) x^\lambda$. One defines an automorphism $\tau^+ \in G^+$ extending τ' by $\tau^+ l = l$ and $\tau^+ e(q) = e(\tau' q)$. It is easily seen that $\tau^+ \in G^+$ and that $\tau \mapsto \tau^+$ is a homomorphism of groups. This is the required splitting. $\square$

2.3 The k -structure on the space of solutions

A **k -structure** on a vector space V over $\bar{k}$ is a k -linear subspace W of V such that $V = \bar{k} \otimes_k W$. Such a k -structure induces a $\text{Gal}(\bar{k}/k)$ -action on V by $\tau(\sum_i f_i w_i) = \sum_i (\tau f_i) w_i$ for $f_i \in \bar{k}$ and $w_i \in W$.

Consider a differential equation M of order d over $k(x)$. Fix an element $a \in k$. This gives an embedding $k(x) \subset k((x-a)) \subset \Omega$ with Ω the universal field of $k((x-a))$. The space of solutions $V = V(M) \subset \Omega$ of M is a vector space over $\bar{k}$ with dimension d . Let G and G^+ be as in Corollary 2.2.7. The space V is invariant under G^+ and the splitting of Corollary 2.2.7 gives an action of $\text{Gal}(\bar{k}/k)$ on V . Let $V_a \subset V$ denote the set of $\text{Gal}(\bar{k}/k)$ -invariant elements.

Lemma 2.3.1 *$V = \bar{k} \otimes_k V_a$ and the action of $\text{Gal}(\bar{k}/k)$ on V is induced by this k -structure on V .*

Proof. We note that any element $\omega \in \Omega$ needs only finitely many elements of $\bar{k}$ for its definition. Hence the subgroup of $\text{Gal}(\bar{k}/k)$ fixing ω is open. Some open normal subgroup N of $\text{Gal}(\bar{k}/k)$ fixes a basis $\{v_1, \dots, v_d\}$ of V . Let W denote the set of N -invariant elements of V and let k' be the field of N -invariant elements of $\bar{k}$. On $W = k'v_1 + \dots + k'v_d$ acts the Galois group $\text{Gal}(k'/k) = \text{Gal}(\bar{k}/k)/N$. For $\tau \in \text{Gal}(k'/k)$ one denotes by $A(\tau) \in \text{Gl}(d, k')$ the matrix which expresses the vectors $\tau(v_1), \dots, \tau(v_d)$ in the basis $\{v_1, \dots, v_d\}$. For $\sigma, \tau \in \text{Gal}(k'/k)$ one finds the formula $A(\sigma\tau) = A(\sigma) \sigma(A(\tau))$. In other words, $\tau \mapsto A(\tau)$ is a 1-cocycle. Its image in $H^1(\text{Gal}(k'/k), \text{Gl}(d, k'))$ is trivial since proposition 3 on page 159 of [Ser68] states that the set $H^1(\text{Gal}(k'/k), \text{Gl}(d, k'))$ is trivial. This means that W also has a basis $w_1, \dots, w_d$ over k' such that $\tau(w_i) = w_i$ for every i . One finds that $W = k' \otimes_k W'$ with $W' := kw_1 + \dots + kw_d$. It follows at once that W' is equal to V_a , the set of $\text{Gal}(\bar{k}/k)$ -invariant elements of V . This proves the lemma. $\square$ A Picard–Vessiot field of the equation M over $k(x)$ is the field $F \subset \Omega$ generated over $\bar{k}(x)$ by a basis of V . The differential Galois group $G(M)$ of

M over $\bar{k}(x)$ is the group of the automorphisms of $F/\bar{k}(x)$ commuting with the differentiation on F . Fix a basis $\{v_1, \dots, v_d\}$ of V_a . Then $G(M)$ can be identified with an algebraic subgroup of $Gl(d, \bar{k})$. This algebraic subgroup is unique up to conjugation with an element in $Gl(d, \bar{k})$. The coordinate ring of $Gl(d, \bar{k})$ is $\bar{k}[X_{i,j}, \frac{1}{D}]$, where $D = \det(X_{i,j})$. Let $I \subset \bar{k}[X_{i,j}, \frac{1}{D}]$ denote the (radical) ideal which defines $G(M)$.

Corollary 2.3.2 *$G(M)$ is defined over the field k .*

Proof. For any $\tau \in Gal(\bar{k}/k)$ and $g \in G(M)$ one has $\tau g \tau^{-1} \in G(M)$. This implies that the ideal I is invariant under τ . A standard argument implies that I is generated by $J := I \cap k[X_{i,j}, \frac{1}{D}]$. Let $G(M)_a$ denote the algebraic group defined by J . Then $G(M) = G(M)_a \otimes_k \bar{k}$. $\square$

2.3.1 Remarks

1. For two elements $a, b \in k$, the k -structures V_a and V_b of V seem to be unrelated. It is not clear how the two groups $G(M)_a$ and $G(M)_b$ are related.
2. The map $\omega : M \mapsto V(M)_a$ from differential equations over $k(x)$ to vector spaces over k commutes with “all constructions of linear algebra”. In more sophisticated terms (see [DM82]) it is a faithful, exact, k -linear, $\otimes$ -functor of the rigid abelian category of left $k(x)[\partial]$ -modules of finite dimension over $k(x)$ to the category of finite dimensional vector spaces over k .

If we restrict ω to the subcategory generated by a fixed M , then it can be seen that the affine group scheme $Aut^\otimes(\omega)$ over k coincides with the algebraic group $G(M)_a$ over k defined above.

3. Let $Z \subset V = V(M)$ be an algebraic subset that is invariant under the differential Galois group $G(M)$ of M . For any $\tau \in Gal(\bar{k}/k)$ the set τZ is again an algebraic subset of V that is invariant under $G(M)$. A case of special interest is Z is a (finite union of) $G(M)$ -invariant subspace.

2.4 Rational solutions of Riccati

One considers a linear homogeneous differential equation of order n over $k(x)$ or $k((x))$. In the first case we fix an $a \in k$ and an embedding $k(x) \subset k((x-a)) \subset \Omega$. This induces the k -structure on the solution space V of the differential equation. In the second case the k -structure on V is given in Section 2.3. The differential

Galois group of the equation is denoted by G . A rational solutions u of the Riccati equation determines a line $\bar{k}y \subset V$, where $y \in V$ satisfies $u = \frac{y'}{y}$, which is invariant under G . Conversely, if $\bar{k}y \subset V$ is a line, invariant under G , then $u = \frac{y'}{y}$ is a rational solution of the Riccati equation. In this section we give estimates for the degree of the field extension of k over which a solution of the Riccati equation is defined.

Lemma 2.4.1 *Suppose that there is a rational solution of the Riccati equation, i.e. a solution in $\bar{k}(x)$ or $\bar{k} \otimes_k k((x))$.*

1. *If there are only finitely many solutions, then each one of them is defined over a field $k' \supset k$ with degree $\leq n$.*
2. *If there are infinitely many solutions of the Riccati equation, then there is a solution which is defined over a field k' with degree $\leq \frac{n}{2}$.*

Proof. For every algebraic character $\chi : G \rightarrow \bar{k}^*$ one defines the vector space $V_\chi := \{v \in V \mid g(v) = \chi(g)v \text{ for all } g \in G\}$. For the χ with $V_\chi \neq 0$ one has $\sum V_\chi \subset V$. Any $\tau \in \text{Gal}(\bar{k}/k)$ acts on the algebraic characters by $\chi \mapsto \tau\chi$ where $\tau\chi(g) = \chi(\tau g \tau^{-1})$. For every non zero V_χ one considers the stabilizer $H \subset \text{Gal}(\bar{k}/k)$ of V_χ . The index of this stabilizer is $\leq \frac{n}{\dim V_\chi}$. Hence V_χ is defined over a field $k' \supset k$ of degree $\leq \frac{n}{\dim V_\chi}$. Inside V_χ one can take a line which is also defined over k' . The solution y corresponding to this line gives a solution $u = \frac{y'}{y}$, which lies in $k'(x)$ or $k'((x))$, of the Riccati equation. If there are only finitely many solutions of the Riccati equation, then all the non-zero V_χ have dimension 1. Hence any choice of of an G -invariant line defines a field extension of degree $\leq n$ over k . In the second case, some V_χ has dimension ≥ 2 . A suitable line in V_χ is therefore defined over a field k' with $[k' : k] \leq \frac{n}{2}$. Furthermore, V_χ contains lines which are defined over arbitrary big extensions of k . $\square$

2.5 Algebraic solutions of the Riccati equation and examples

One considers as before a differential equation over the field K which is either $k(x)$ or $k((x))$. The vector space V over $\bar{k}$ of solutions is given a k -structure as in section 2.3. The differential Galois group is called G .

A solution $u = \frac{y'}{y}$ of the Riccati equation, algebraic of degree m , corresponds to a line $L = \bar{k}y \subset V$ such that its stabilizer $H \subset G$ is a subgroup of index m . The element u satisfies a monic irreducible equation P of degree m over $\bar{k}K$. The collection of all zeroes of P corresponds to the orbit GL of the line L . We want to find the smallest field extension k' of k such that the coefficients of P are in

$k'K$. This is equivalent to finding the smallest field extension $k' \supset k$ such that the orbit GL is defined over k .

Let us define **an m -line** to be a G -invariant subset of V consisting of m lines through 0, such that G acts transitively on the m lines. The collection of all m -lines is denoted by $\mathcal{L}_m$. This set can be infinite.

Let us define **an m -group** to be the conjugacy class $[H]$ of an algebraic subgroup H of index m such that H is the stabilizer of at least one line in V . The collection of all m -groups is denoted by $\mathcal{H}_m$. This set is finite.

The map $\phi : \mathcal{L}_m \rightarrow \mathcal{H}_m$ is defined as follows. The image of an m -line $L_1 \cup \dots \cup L_m$ is the conjugacy class of the stabilizer of L_1 (or any L_i). The map ϕ is by definition surjective. More precisely, let H be an algebraic subgroup of index m such that the collection

$$X := \{L \mid L \text{ is a line with stabilizer } gHg^{-1} \text{ for some } g \in G\}$$

is not empty. Then $\phi^{-1}([H])$ is the set of G -orbits of X .

On $\mathcal{L}_m$ the Galois group $Gal(\bar{k}/k)$ acts in the obvious way. On $\mathcal{H}_m$ we let any $\tau \in Gal(\bar{k}/k)$ act by $\tau([H]) = [\tau^{-1}H\tau]$. The map ϕ is equivariant for the defined actions.

Proposition 2.5.1 *Let u be an algebraic solution of the Riccati equation and let k' be the minimal extension of k such that the minimal monic equation of u over $\bar{k}K$ is defined over $k'K$. Let L be the line in V corresponding to u and let $H \subset G$ denote the stabilizer of L . Then*

$$[k' : k] \leq (\#Gal(\bar{k}/k)[H])(\#\phi^{-1}([H]))$$

Proof. Since k' is also the minimal extension for which the m -line $[L] := GL$ is defined over k' , the inequality follows at once from the obvious inequality

$$(\#Gal(\bar{k}/k)[L]) \leq (\#Gal(\bar{k}/k)[H])(\#\phi^{-1}([H])).$$

□

Remark 2.5.2 *For $m = 1$ the last proposition gives the inequality*

$$[k' : k] \leq \text{the number of lines fixed by } G.$$

This is in accordance with lemma 2.4.1.

2.5.1 Equations of order two

One considers an equation of order two over the field $k(x)$. This equation can be normalized and has then the form $y'' = ry$, with $r \in k(x)$. The corresponding Riccati equation is $u' + u^2 = r$. The differential Galois group G is an algebraic subgroup of $Sl(2, \bar{k})$ and is unique up to conjugation. According to [Kov86] one has the following result:

Theorem 2.5.3 *The following statements hold.*

1. *If there is no algebraic solution over $\bar{k}(x)$ of the Riccati equation, then $G = Sl(2, \bar{k})$.*
2. *If there is an algebraic solution of the Riccati equation, then the minimal degree m of such an equation can be 1, 2, 4, 6, 12 and*

(a) *If $m = 1$ then $G \subset \left\{ \begin{pmatrix} c & d \\ 0 & c^{-1} \end{pmatrix} \mid c \in \bar{k}^*, d \in \bar{k} \right\}$.*

(b) *If $m = 2$ then $G = D_\infty$ or $G = D_n$ with $n \geq 3$. (The dihedral groups).*

(c) *If $m = 4$ then G is the tetrahedral group.*

(d) *If $m = 6$ then G is the octahedral group.*

(e) *If $m = 12$ then G is the icosahedral group.*

Using the inequality in Proposition 2.5.1 and Lemma 2.4.1 one finds

Theorem 2.5.4 *Assume that the Riccati equation $u' + u^2 = r \in k(x)$ has a solution which is algebraic over $\bar{k}(x)$. Let m be the minimal degree, as in Theorem 2.5.3. Then the coefficients of the monic minimal polynomial of u over $\bar{k}(x)$ lie in a field $k'(x)$ with $[k' : k] \leq 3$. More precisely:*

1. *If $m = 1$ and G is the multiplicative group G_m or a finite cyclic group of order > 2 then $[k' : k] \leq 2$.*
2. *If $m = 2$ and $G = D_4$, then $[k' : k] = 3$ or $k' = k$.*
3. *If $m = 4$ and G is the tetrahedral group, then $[k' : k] \leq 2$.*
4. *In all other cases $k' = k$.*

Proof. We will give the proof case by case.

1. If $m = 1$ and there are infinitely many solutions or precisely one solution of Riccati in $\bar{k}(x)$, then by Lemma 2.4.1 one has $k' = k$. In the remaining case $[k' : k] \leq 2$.
2. If $m = 2$ and $G \neq D_4$, then G has precisely one algebraic subgroup H of index 2. Hence $\#Gal(\bar{k}/k)[H] = 1$. Further $\#\phi^{-1}([H]) = 1$.

3. If $m = 2$ and $G = D_4$, then $\mathcal{H}_2$ has three elements. For each such $[H] \in \mathcal{H}_2$ one has $\#\phi^{-1}([H]) = 1$.
4. For the tetrahedral group one has $\#\mathcal{H}_4 = 1$ and $\#\phi^{-1}([H]) = 2$.
5. For the octahedral group one has $\#\mathcal{H}_6 = 1$ and $\#\phi^{-1}([H]) = 1$.
6. For the icosahedral group one has $\#\mathcal{H}_{12} = 1$ and $\#\phi^{-1}([H]) = 1$.

□

2.5.2 Equations of order three

A third-order equation can be normalized in the form $y''' + py' + qy = 0$ with $p, q \in k(x)$. The differential Galois group G is an algebraic subgroup of $Sl(3, \bar{k})$. The Riccati equation reads $u'' + 3uu' + u^3 + pu + q = 0$. The analogue Theorem 2.5.5 of Theorem 2.5.3 is proved in [SU93]. We will use their terminology and description of finite primitive groups. In particular, a subgroup H of $Sl(3, \bar{k})$ is called **1-reducible** if the elements of H have a common eigenvector.

Theorem 2.5.5 *The following statements hold.*

1. *If there is no algebraic solution over $\bar{k}(x)$ of the Riccati equation then G satisfies one of the following properties:*
 - (a) $G = Sl(3, \bar{k})$;
 - (b) $G/Z(G) = PSL(2, \bar{k})$ where $Z(G)$ denotes the center of G ;
 - (c) G is reducible but not 1-reducible.
2. *If there is an algebraic solution of the Riccati equation then the minimal degree m of such an equation can be 1, 3, 6, 9, 21, 36 and*
 - (a) *If $m = 1$ then G is a 1-reducible group.*
 - (b) *If $m = 3$ then G is an imprimitive group.*
 - (c) *If $m = 6$ then $G/Z(G)$ is isomorphic to F_{36} or A_5 .*
 - (d) *If $m = 9$ then $G/Z(G)$ is isomorphic to H_{72} or H_{216} .*
 - (e) *If $m = 21$ then $G/Z(G) = G_{168}$.*
 - (f) *If $m = 36$ then $G/Z(G) = A_6$.*

Using Lemma 2.4.1 and Proposition 2.5.1 one finds

Theorem 2.5.6 *Suppose that the Riccati equation has an algebraic solution and let m be as in Theorem 2.5.5. There exists an algebraic solution of the Riccati equation of degree m such that the coefficients of the monic minimal equation over $\bar{k}(x)$ lie in $k'(x)$ with*

1. $[k' : k] \leq 3$ if the equation is 1-reducible.
2. $[k' : k] \leq 4$ if G is imprimitive.
3. $[k' : k] \leq 2$ in case $G/Z(G) = F_{36}$.
4. $k' = k$ in all other cases.

Proof.

1. If G is 1-reducible one applies lemma 2.4.1 and thus part (1) of the theorem is proved.
2. Let G be imprimitive. A system of imprimitivity consists of three lines $\bar{k}e_i$; $i = 1, 2, 3$ such that $\{e_1, e_2, e_3\}$ is a basis of the solution space V and such that G permutes the three lines. In particular, this is a 3-line for G . If G has only one system of imprimitivity then this system is defined over k and $k' = k$ holds.

If there is more than one system of imprimitivity then one easily sees that $G^o = 1$ and the group G is finite. In particular, G is completely reducible. For any 3-line $\{L_1, L_2, L_3\}$ for G the space $L_1 + L_2 + L_3 \subset V$ is G -invariant. If this space has dimension 2 then G has also a one-dimensional invariant subspace. This contradicts our assumption. Hence $\mathcal{L}_3$ is the set of all systems of imprimitivity of G . According to [Bli17] there are at most four systems of imprimitivity or in our language $\#\mathcal{L}_3 \leq 4$. This proves part (2) of the theorem. We remark that, according to Blichtfeldt (1917), there are only two imprimitive groups with four systems of imprimitivity. The groups have orders 27 and 54 respectively. The corresponding subgroups of $PGL(3)$ have orders 9 and 18. They are sometimes called H_9 and H_{18} .

3. Suppose now that G is a finite primitive group and m the number defined in theorem 2.5.5. Using the description of such groups given in [SU93], one can verify that any 1-reducible subgroup H of index m in G is non-abelian. Therefore H can only fix one line L in the solution space V . It follows that $[H]$ (the set of conjugates of H in G) consists of m elements. Moreover, for any $[H] \in \mathcal{H}_m$ the set $\phi^{-1}([H])$ consists of one element. Therefore $[k' : k] \leq \#\mathcal{H}_m = \frac{1}{m}\#T$, where T denotes the set of 1-reducible subgroups of index m in G . Counting gives $\#T = m$ except in one case. This is the case $G/Z(G) = F_{36}$. In this case, $m = 6$ and $\#T = 12$. This proves parts (3) and (4) of the theorem.

□

2.5.3 Remarks

1. Consider a differential equation of order n over the field $K = k((x))$. According to [Lev75], there is a field extension $K' \supset K$ of degree $\leq n$ such that the equation over K' has a one-dimensional factor. Let e denote the ramification index of K' over K and f the degree of the residue field extension. Then $ef = [K' : K] \leq n$. The extension $K' \subset K'(x^{\frac{1}{e}})$ is unramified and has degree $\leq n$. This can be reformulated as follows:

The minimal number m such that the Riccati equation has a solution u which is algebraic over $\bar{k}K$ is $\leq n$. The minimal monic equation of u over $\bar{k}K$ has its coefficients in a field $k'K$ with $[k' : k] \leq n$.

2. Let k be a subfield of the field of complex numbers. Then we replace the field of formal Laurent series, used in remark (1) above, by the field K of convergent Laurent series. Let G be the differential Galois group of the equation of order n and let G^o be the component of 1 in G . One knows that the group G/G^o does not change if one makes the step from convergent Laurent series to formal Laurent series. This implies that this group is cyclic. We note that there are in general no algebraic solutions of the Riccati equation!

Any algebraic solution u of the Riccati equation corresponds to a line in the solution space with stabilizer $H \supset G^o$.

The group H is uniquely determined by its index in G and in particular invariant under conjugation with any element in $\text{Gal}(\bar{k}/k)$. Using Lemma 2.4.1 one finds the following:

If the Riccati equation has an algebraic solution then there is an algebraic solution u such that its monic minimal equation over the field $\bar{k}K$ has coefficients in a field $k'K$ with $[k' : k] \leq n$.

2.6 Symmetries

The aim of this section is to construct differential equations over the field $k(x)$ such that the algebraic solutions of degree m of the corresponding Riccati equation are defined over a proper extension of the base field k . There are two ingredients in the construction:

1. The group of symmetries of the equation.
2. Forms of a differential equation over $k(x)$.

Let k be a field of characteristic 0 with algebraic closure $\bar{k}$. The ring of differential operators $k(x)[\partial_x]$ is the skew polynomial ring defined by the relation $\partial_x x = x\partial_x + 1$. We note that $k(x)$ is the unique maximal subfield of $k(x)[\partial_x]$.

Lemma 2.6.1 *The k -algebra homomorphisms $\phi : k(x)[\partial_x] \rightarrow k(t)[\partial_t]$ are given by*

$$\phi(x) = a \text{ and } \phi(\partial_x) = \frac{1}{a'}\partial_t + b$$

with $a \in k(t) \setminus k$; $a' := \frac{d}{dt}a$ and $b \in k(t)$.

Proof. ϕ is determined by $\phi(x)$ and $\phi(\partial_x)$. These two elements of $k(t)[\partial_t]$ satisfy the relation $\phi(\partial_x)\phi(x) - \phi(x)\phi(\partial_x) = 1$. A straightforward calculation with this relation yields the lemma. $\square$

Corollary 2.6.2 *Let $\text{Aut}(k(x)[\partial_x])$ denote the group of the k -algebra automorphisms of $k(x)[\partial_x]$. There is a split exact sequence of groups*

$$0 \rightarrow k(x) \rightarrow \text{Aut}(k(x)[\partial_x]) \rightarrow \text{PGL}(2, k) \rightarrow 1$$

Proof. The element $a = \phi(x)$ must satisfy $k(x) = k(a)$. Therefore, any automorphism ϕ induces an automorphism of $k(x)$. This explains the map of $\text{Aut}(k(x)[\partial_x]) \rightarrow \text{PGL}(2, k)$. Clearly this map is surjective and the kernel consists of the automorphisms ϕ with $\phi(x) = x$ and $\phi(\partial_x) = \partial_x + b$ where $b \in k(x)$ is arbitrary. The splitting s is given by: if $\sigma \in \text{PGL}(2, k)$ then $s(\sigma)(x) = \sigma(x)$ and $s(\sigma)(\partial_x) = \frac{1}{\sigma(x)'}\partial_x$. This proves the corollary. $\square$

2.6.1 Symmetries of L

Let $L \in k(x)[\partial_x] \setminus k(x)$. The group $\text{Sym}_k(L)$ of the symmetries of L consists of the automorphisms ϕ of $k(x)[\partial_x]$ satisfying $\phi(L) = L$. The map $\text{Sym}_k(L) \rightarrow \text{PGL}(2, k)$ is injective as one easily sees.

In some interesting cases L itself has very few symmetries but there is a non-trivial finite group H of automorphisms ϕ of $k(x)[\partial_x]$ satisfying $\phi(L) = fL$ for some $f \in k(x)^*$. In this situation one can change L into gL for a certain $g \in k(x)^*$ such that H is contained in the group of symmetries of gL . We will call this *normalizing* L . That normalization is always possible can be seen as follows:

Write $f(\phi)$ for the element of $k(x)^*$ satisfying $\phi(L) = f(\phi)L$. Then $\phi \in H \mapsto f(\phi) \in k(x)^*$ is a 1-cocycle. The corresponding cohomology group is $H^1(H, k(x)^*)$. We will show that this group is trivial. Indeed, let $K \subset k(x)$ denote the subfield of the H -invariant elements of $k(x)$. Then $K \subset k(x)$ is a Galois extension with Galois group H . By Hilbert 90 the group $H^1(H, k(x)^*) = 1$. Therefore the 1-cocycle $\phi \mapsto f(\phi)$ is trivial. This implies that we can choose a

$g \in k(x)^*$ such that $\phi(gL) = gL$ for every $\phi \in H$.

In general, the group of symmetries of an operator L is trivial. In many cases a study of the singular points of the operator shows that this group is a finite subgroup of $PGL(2, k)$.

We will explain this and introduce some terminology. Let the operator L have the form $f(\partial_x^n + a_{n-1}\partial_x^{n-1} + \dots + a_0)$. Then $p \in \bar{k}$ is called a *singularity of L* if some a_i has a pole at p . The point $p = \infty$ is called a singular point if L expressed in the local parameter $t = x^{-1}$ is singular for $t = 0$. We note that an automorphism ϕ of $k(x)[\partial_x]$ not only changes the position of the singular points but singularities can disappear and new ones can appear. We introduce the notion of *essential singularity* in order to distinguish among the singular points.

A singular point $p \in \bar{k} \cup \{\infty\}$ of L is called **essential** if there is no automorphism ϕ , with $\phi(x) = x$, such that p is a regular point of $\phi(L)$.

If p is an essential singular point of L then $\phi(p)$ is an essential singular point of $\phi(L)$. Indeed, it suffices to verify this statement for three types of automorphisms:

1. $\phi(x) = x$. By definition, this ϕ preserves the essential singular points.
2. $\phi(x) = x + \lambda$ with $\lambda \in k$ and $\phi(\partial_x) = \partial_x$. This case is trivial.
3. $\phi(x) = x^{-1}$ and $\phi(\partial_x) = -\frac{1}{x^2}\partial_x$. One can verify the statement by hand.

One can explain the notion of essential singularity as follows. Let $L = f(\partial_x^n + a_{n-1}\partial_x^{n-1} + \dots + a_0)$ be a differential operator and let $p \in \bar{k}$. We perform on L the following operation: first, delete the term f ; second, make the unique transformation $x \mapsto x$ and $\partial_x \mapsto \partial_x - \frac{a_{n-1}}{n}$ which kills the coefficient of ∂_x^{n-1} of L . The result is the differential operator $M = \partial^n + b_{n-2}\partial_x^{n-2} + \dots + b_0$. It is not difficult to see that L has an essential singularity at p if and only if p is a pole of some of the b_i .

Any L has only finitely many essential singular points. If this number is ≥ 3 then $Sym_k(L)$ is obviously a finite group.

Let H be a finite group of automorphisms of $k(x)[\partial_x]$. The set of H -invariant elements of $k(x)[\partial_x]$ can be identified with $k(t)[\partial_t]$. Indeed, choose t such that $k(t)$ is the subfield of $k(x)$ consisting of the H -invariant elements. One can choose $b \in k(x)$ such that $\partial_x := \frac{1}{t}\partial_t + b$ is H -invariant. This follows from $H^1(H, k(x)) = 0$. Let $\phi : k(t)[\partial_t] \rightarrow k(x)[\partial_x]$ denote the inclusion. A differential operator $L \in k(x)[\partial_x]$ has H as group of symmetries, if and only if $L = \phi(M)$ for some $M \in k(t)[\partial_t]$.

This shows that any finite subgroup of $PGL(2, k)$ occurs as group of symmetries of some differential operator.

2.6.2 Transforming algebraic solutions of Riccati

Let $L \in k(x)[\partial_x] \setminus k(x)$ and a k -algebra homomorphism $\phi : k(x)[\partial_x] \rightarrow k(t)[\partial_t]$ be given. We extend ϕ to a morphism of $\bar{k}(x)[\partial_x] \rightarrow \bar{k}(t)[\partial_t]$ by extending the homomorphism of fields $k(x) \rightarrow k(t)$ to the algebraic closures $\bar{k}(x)$ and $\bar{k}(t)$ of those fields. An algebraic solution $u \in \bar{k}(x)$ of the Riccati equation means that L factors as $M(\partial_x - u)$ in $\bar{k}(x)[\partial_x]$. Then $\phi(L)$ factors as $\phi(M)(\phi(\partial_x) - \phi(u))$. Write $\phi(\partial_x) = \frac{1}{\phi(x)}\partial_t + b$, then $\phi(x)'(\phi(u) - b)$ is a solution of the Riccati equation of $\phi(L)$.

Let $P(x, T) \in \bar{k}(x)[T]$ be the monic irreducible polynomial of degree m satisfied by u then $\phi(x)'(\phi(u) - b)$ satisfies the monic polynomial $(\phi(x)')^m P(\phi(x), \frac{1}{\phi(x)}T + b)$ over $\bar{k}(t)$. We will denote this polynomial by ϕ_*P .

Let G be a group of symmetries of L . Suppose that the collection $\mathcal{R}_m(L)$ of the algebraic solutions of degree m over $\bar{k}(x)$ of the Riccati equation is finite. Then there are distinct monic irreducible polynomials $P_i(x, T)$; $1 \leq i \leq s$ of degree m over $\bar{k}(x)$ such that $\mathcal{R}_m(L)$ is equal to the set of solutions of $P_1 \dots P_s$. For every $g \in G$ and i the polynomial g_*P_i belongs to $\{P_1, \dots, P_s\}$. Hence G acts as a group of permutations on $\{P_1, \dots, P_s\}$.

2.6.3 Forms of a differential operator

Let $L \in k(x)[\partial_x] \setminus k(x)$ be a differential operator. A differential operator $M \in k(x)[\partial_x]$ of the form $M = \phi(L)$ with $\phi \in \text{Aut}(\bar{k}(x)[\partial_x])$ is called a **form** of L . Two forms M_1, M_2 are equivalent if there exists a $\psi \in \text{Aut}(k(x)[\partial_x])$ with $\psi(M_1) = M_2$.

We let the group $\text{Gal}(\bar{k}/k)$ act on $\bar{k}(x)[\partial_x]$ by its natural action on $\bar{k}$ and as the identity on $k(x)[\partial_x]$. Further $\text{Gal}(\bar{k}/k)$ acts on $\text{Sym}_{\bar{k}}(L)$ by $\tau(g) = \tau g \tau^{-1}$ (with $\tau \in \text{Gal}(\bar{k}/k)$ and $g \in \text{Sym}_{\bar{k}}(L)$). In the following we will construct an injective map $\alpha : \text{Forms}(L) \rightarrow H^1(\text{Gal}(\bar{k}/k), \text{Sym}_{\bar{k}}(L))$, where $\text{Forms}(L)$ is the set of equivalence classes of forms of L .

For a form $M = \phi(L)$ of L and a $\tau \in \text{Gal}(\bar{k}/k)$ one has that $a(\tau) := \phi^{-1}\tau\phi\tau^{-1} \in \text{Sym}_{\bar{k}}(L)$. Moreover $\tau \mapsto a(\tau)$ is a 1-cocycle, i.e. $a(\tau_1\tau_2) = a(\tau_1)\tau_1(a(\tau_2))$ for all $\tau_1, \tau_2 \in \text{Gal}(\bar{k}/k)$. The class of $\tau \mapsto a(\tau)$ in $H^1(\text{Gal}(\bar{k}/k), \text{Sym}_{\bar{k}}(L))$ does not depend on the choice of ϕ . Indeed, any other choice for ϕ has the form ϕg with $g \in \text{Sym}_{\bar{k}}(L)$. The new 1-cocycle has the form $\tau \mapsto g^{-1}\phi^{-1}\tau\phi g\tau^{-1} = g^{-1}(\phi^{-1}\tau\phi\tau^{-1})\tau g\tau^{-1}$. By definition this is an equivalent 1-cocycle. We will verify that the resulting map $\alpha : \text{Forms}(L) \rightarrow H^1(\text{Gal}(\bar{k}/k), \text{Sym}_{\bar{k}}(L))$ is injective. In general α will not be surjective. Consider the following two maps:

$$\beta : H^1(\text{Gal}(\bar{k}/k), \text{Sym}_{\bar{k}}(L)) \rightarrow H^1(\text{Gal}(\bar{k}/k), \text{Aut}(\bar{k}(x)[\partial_x]))$$

$$\gamma : H^1(\text{Gal}(\bar{k}/k), \text{Aut}(\bar{k}(x)[\partial_x])) \rightarrow H^1(\text{Gal}(\bar{k}/k), \text{PGL}(2, \bar{k}))$$

The trivial element of those sets (i.e. the image of the trivial 1-cocycle) is denoted by 1.

Lemma 2.6.3 *The following statements hold.*

1. α is injective.
2. The image of α is $\beta^{-1}(\{1\})$.
3. γ is surjective.
4. $\gamma^{-1}(\{1\}) = \{1\}$.
5. α is bijective if either $H^1(\text{Gal}(\bar{k}/k), \text{PGL}(2, \bar{k}))$ is trivial or if the subgroup $\text{Sym}_{\bar{k}}(L)$ of $\text{PGL}(2, \bar{k})$ lifts to a subgroup of $\text{GL}(2, \bar{k})$.

Proof. We will prove this theorem case by case.

1. If the $M_i = \phi_i(L)$ for $i = 1, 2$ induce the same element of $H^1(\text{Gal}(\bar{k}/k), \text{Sym}_{\bar{k}}(L))$, then there is a $g \in \text{Sym}_{\bar{k}}(L)$ with

$$\phi_2^{-1}\tau\phi_2\tau^{-1} = g^{-1}(\phi_1^{-1}\tau\phi_1\tau^{-1})\tau g\tau^{-1},$$

for all $\tau \in \text{Gal}(\bar{k}/k)$. This implies that $\phi_1 g \phi_2^{-1} \tau = \tau \phi_1 g \phi_2^{-1}$ for all τ and so $\phi_1 g \phi_2^{-1} \in \text{Aut}(k(x)[\partial_x])$. Then $\phi_1 g \phi_2^{-1}(M_2) = M_1$ proves that M_1 and M_2 are equivalent.

2. Clearly, the image of $\beta\alpha$ is $\{1\}$. On the other hand, let a be a 1-cocycle for $\text{Sym}_{\bar{k}}(L)$ with $\beta(a) = 1$. Then there exists a $\phi \in \text{Aut}(\bar{k}(x)[\partial_x])$ with $a(\tau) = \phi^{-1}\tau(\phi) = \phi^{-1}\tau\phi\tau^{-1}$ for all $\tau \in \text{Gal}(\bar{k}/k)$. Put $M := \phi(L)$. Then $\tau(M) = \tau\phi\tau^{-1}(L) = \phi a(\tau)(L) = \phi(L) = M$. Hence $M \in k(x)[\partial_x]$ is a form of L and M induces the 1-cocycle a .
3. This follows from the splitting of the group homomorphism $\text{Aut}(\bar{k}(x)[\partial_x]) \rightarrow \text{PGL}(2, \bar{k})$.
4. Let a be a 1-cocycle for $\text{Sym}_{\bar{k}}(L)$ which has trivial image in $H^1(\text{Gal}(\bar{k}/k), \text{PGL}(2, \bar{k}))$. Then a is equivalent to a 1-cocycle for the normal subgroup $\bar{k}(x)$ of $\text{Aut}(\bar{k}(x)[\partial_x])$. Since $\bar{k}(x) = \bar{k} \otimes_k k(x)$ one has that $H^1(\text{Gal}(\bar{k}/k), \bar{k}(x)) = 0$. Hence a is a trivial 1-cocycle.
5. This follows from statements (1)-(4) and the well known fact that $H^1(\text{Gal}(\bar{k}/k), \text{GL}(2, \bar{k})) = 1$.

□

2.6.4 Construction of special differential equations

One fixes a differential equation $L \in k(x)[\partial_x]$ and a number $m \geq 1$. One assumes that the set $\mathcal{R}_m(L)$, as defined in Section 2.6.2, is finite and that the monic polynomials $P_1, \dots, P_s$ actually lie in $k(x)[T]$.

Let $G \subset \text{Sym}_k(L)$ be some finite group which lifts to a subgroup of $\text{Gl}(2, k)$. This group acts as a permutation group on $\{P_1, \dots, P_s\}$.

Let $h : \text{Gal}(\bar{k}/k) \rightarrow G$ be a continuous homomorphism. Then one can see h as an element of $H^1(\text{Gal}(\bar{k}/k), \text{Sym}_{\bar{k}}(L))$. There is an automorphism ϕ of $\bar{k}(x)[\partial_x]$ such that $M := \phi(L) \in k(x)[\partial_x]$ such that $\tau\phi = \phi h(\tau)\tau$ for all $\tau \in \text{Gal}(\bar{k}/k)$.

The set $\{\phi_*P_1, \dots, \phi_*P_s\}$ are the monic irreducible polynomials of degree m over $\bar{k}(x)$ with as set of zeroes all the solutions of the Riccati equation of M which are algebraic over $\bar{k}(x)$ of degree m . Since $\tau\phi = \phi h(\tau)\tau$ and $\tau P_i = P_i$ for all τ , one finds that $\tau \in \text{Gal}(\bar{k}/k)$ permutes the set $\{\phi_*P_1, \dots, \phi_*P_s\}$ in the same way as $h(\tau)$ permutes the $\{P_1, \dots, P_s\}$. We can formulate the results above as follows.

Theorem 2.6.4 *Let $L \in k(x)[\partial_x]$ be a differential equation with a finite group of symmetries $G \subset \text{Sym}_k(L)$ which lifts to a subgroup of $\text{Gl}(2, k)$. Let $m \geq 1$ and suppose that the set of algebraic solutions of degree m over $\bar{k}(x)$ of the Riccati equation of L is finite and given as the set of zeroes of $P_1 \dots P_s$ where the $P_i \in k(x)[T]$ are distinct monic polynomials of degree m and irreducible as elements of $k(x)[T]$. Let a continuous homomorphism $h : \text{Gal}(\bar{k}/k) \rightarrow G$ be given. Then there is a form $M = \phi(L) \in k(x)[\partial_x]$ of L with $\tau\phi = \phi h(\tau)\tau$ for all $\tau \in \text{Gal}(\bar{k}/k)$. The polynomials $Q_i := \phi_*P_i \in \bar{k}(x)[T]$; $1 \leq i \leq s$ are monic and irreducible. The set of zeroes of $Q_1 \dots Q_s$ coincides with the set of algebraic solutions of degree m over $\bar{k}(x)$ of the Riccati equation of M . The action of $\text{Gal}(\bar{k}/k)$ on $\{Q_1, \dots, Q_s\}$ coincides with the homomorphism $\text{Gal}(\bar{k}/k) \xrightarrow{h} G \rightarrow \text{Perm}(\{P_1, \dots, P_s\})$, where $\text{Perm}(\{P_1, \dots, P_s\})$ denotes the group of permutations of $\{P_1, \dots, P_s\}$.*

2.6.5 Examples

We will give here examples to show that the inequalities in Theorem 2.5.4 and Theorem 2.5.6, part 1 are sharp.

Cyclic groups

Consider the differential operator $L = (x\partial_x)^2 - a$ with $a \in k^*$. There are two singular points 0 and ∞ . They are essential singular points. The symmetry group of L is the group of all the $\phi \in \text{PGL}(2, \bar{k})$ for which $\{0, \infty\}$ is invariant. In particular, ϕ given by $\phi(x) = x^{-1}$ and $\phi(x\partial_x) = -x\partial_x$, is a symmetry. The two solutions of the Riccati equation (with respect to $' = x\frac{d}{dx}$) are $\pm\sqrt{a}$. The symmetry ϕ permutes these two solutions.

1. If $\sqrt{a} \notin \mathbf{Q}$ then the differential Galois group is $\mathbf{G}_m$. If, moreover, $\sqrt{a} \notin k$ then the Riccati equation defines a degree two extension of k .
2. If $(\frac{t}{n})^2 = a$ with $t, n \in \mathbf{Z}, t, n \geq 1$ and relative prime, then the differential Galois group is cyclic of order n . The two solutions of the Riccati equation are in $k(x)$ and since they are permuted by ϕ , one can apply Theorem 2.6.4. Hence there is for every quadratic extension $k' \supset k$ a form M of L such that the solutions of the Riccati equation of M are in $k'(x) \setminus k(x)$. In the next subsection, we will give an explicit example M .

Cyclic groups again

Let $k' = k(\lambda)$ with $\lambda^2 \in k$ and $\lambda \notin k$. Take $u_0, u_1 \in k(x)$ and $u_1 \neq 0$ and write $u = u_0 + \lambda u_1$. The equation $r = u' + u^2 \in k(x)$ is equivalent to $u_0 = -1/2 \frac{u_1'}{u_1}$ and $r = u_0^2 + u_0' + \lambda^2 u_1^2$. Clearly $u_0 + \lambda u_1$ and $u_0 - \lambda u_1$ are two solutions of the Riccati equation of $y'' = ry$. The equation $y' = (-1/2 \frac{u_1'}{u_1} + \lambda u_1)y$ has a differential Galois group (over $k'(x)$ or $\bar{k}(x)$) which can be finite or the multiplicative group $\mathbf{G}_m$. For a general choice of $u_1 \in k(x)$ the differential Galois group will be $\mathbf{G}_m$.

If one chooses $u_1 = \frac{a}{b(x^2 - \lambda^2)}$ with $a, b \in \mathbf{Z} \setminus 0$, $b > 1$ and $\text{g.c.d.}(a, b) = 1$ then $y = (x - \lambda)^{(\frac{1}{2} + \frac{a}{2b})} (x + \lambda)^{(\frac{1}{2} - \frac{a}{2b})}$ satisfies the equation $y' = (-1/2 \frac{u_1'}{u_1} + \lambda u_1)y$. Therefore the differential Galois group has order b if a, b are odd and has order $2b$ if a or b is even.

The group D_4

The standard differential operator for this group is (see [BD79] with in their notation the case $e_1 = e_2 = e_3 = 2$)

$$L = \partial_x^2 - \left(\frac{3}{16x(x-1)} - \frac{3}{16x^2} - \frac{3}{16(x-1)^2} \right)$$

The singular points are $\{0, 1, \infty\}$. They are essential singular points. The symmetry group of L is therefore contained in the subgroup of $PGL(2, \mathbf{Q})$ which leaves $\{0, 1, \infty\}$ invariant. This group is isomorphic to S_3 and lifts to a subgroup of $Gl(2, \mathbf{Q})$.

The operator L is actually not invariant under S_3 . One has to normalize L into $x^2(1 - x^2)L$. The latter has S_3 as group of symmetries. One can calculate that $u = \frac{3x-1+\sqrt{x}}{4x(x-1)}$ is a solution of the Riccati equation. The corresponding field extension of $\mathbf{Q}(x)$ is $\mathbf{Q}(\sqrt{x})$. The other solutions of the Riccati equation give the field extensions $\mathbf{Q}(\sqrt{x-1})$ and $\mathbf{Q}(\sqrt{x(x-1)})$. It follows that the six

quadratic solutions of the Riccati are the roots of three irreducible monic polynomials $P_1, P_2, P_3 \in \mathbf{Q}(x)[T]$ and that the symmetry group of L acts as S_3 on $\{P_1, P_2, P_3\}$. Hence we can apply Theorem 2.6.4. Consider L as given over some field $k \supset \mathbf{Q}$ and let $k' \supset k$ be a Galois extension with Galois group isomorphic to S_3 . Then there is a form M of L with coefficients in $k(x)$ such that the Galois group $\text{Gal}(k'/k)$ acts as S_3 on $\{Q_1, Q_2, Q_3\}$, where the Q_i are the monic irreducible polynomials of degree 2 over $\bar{k}(x)$ which have as zeroes the six solutions of the Riccati equation of M . The minimal field $k_i \supset k$ such that $Q_i \in k_i(x)[T]$ has degree 3 over k .

One can make this example more explicit as follows. Write $k' = k(a_1, a_2, a_3)$ such that the Galois group of k'/k acts as S_3 on $\{a_1, a_2, a_3\}$. Let the equation of the a_i over k be $X^3 - e_1X^2 + e_2X - e_3 = 0$. Define $\phi : \bar{k}(x)[\partial_x] \rightarrow \bar{k}(x)[\partial_x]$ by $\phi(x) = \frac{a_2 - a_3}{a_2 - a_1} \frac{x - a_1}{x - a_3}$ and a suitable $\phi(\partial_x)$ such that $\phi(L)$ takes the form $f(\partial_x^2 - r)$ for some $f, r \in \bar{k}(x)$. The term f disappears after a normalization of L . A long calculation yields the expression for r :

$$\frac{3}{16} \frac{(3e_1e_3 - e_2^2) + (e_1e_2 - 9e_3)x + (3e_2 - e_1^2)x^2}{(x^3 - e_1x^2 + e_2x - e_3)^2}$$

The special choice: a_1, a_2, a_3 are the three roots of $X^3 - 2$, gives the nice equation $\partial_x^2 + \frac{27x}{8(x^3-2)^2}$. The Galois group of $F := \mathbf{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$ acts as the group S_3 on the three quadratic irreducible minimal polynomials $\{Q_1, Q_2, Q_3\} \subset F(x)[T]$ corresponding to six quadratic solutions of the Riccati equation.

The tetrahedral group

The standard example for the tetrahedral group is the differential operator (See [BD79] with in their notation $e_1 = 2, e_2 = e_3 = 3$).

$$L := \partial_x^2 - \left(\frac{3}{16x(x-1)} - \frac{3}{16x^2} - \frac{2}{9(x-1)^2} \right)$$

The three singular points $\{0, 1, \infty\}$ are essential singular points. Any symmetry of L has to permute those three points. Further the singularities at 0 and 1 are isomorphic and the singularity at ∞ is not isomorphic to the one at 0. Therefore the only symmetry, $\neq 1$, is g given by $g(x) = \frac{x}{x-1}$ and $g(\partial_x) = -(x-1)^2\partial_x + (x-1)$. Actually, one has to normalize L into x^4L and then $g(x^4L) = x^4L$. We note that [BD79] contains a mistake at this point. There are eight algebraic solutions of degree 4 of the Riccati equation and there are two irreducible monic polynomials $P_1, P_2 \in \overline{\mathbf{Q}}(x)[T]$ of degree 4 such that the set of zeros of P_1P_2 is the set of those eight solutions. Actually, one of the polynomials, say P_1 , is computed in [Kov86]. This polynomial turns out to lie in $\mathbf{Q}(x)[T]$. A calculation shows that $g_*P_1 \neq P_1$

and so $g_*P_1 = P_2$. Therefore $P_1, P_2 \in \mathbf{Q}(x)[T]$ and g permutes them. It seems possible to make a proof of this without the explicit knowledge of P_1 .

Applying Theorem 2.6.4, one finds a form $\phi(M)$ of L over k and a quadratic extension $k' \supset k$ such that the Galois group of k'/k permutes the corresponding polynomials $\{\phi_*P_1, \phi_*P_2\}$ of M . Let $k' = k(\lambda)$ with $\lambda^2 \in k$ and $\lambda \notin k$. Then one can take for ϕ the automorphism given by $\phi(x) = \frac{2}{1+2\lambda x}$ and suitable $\phi(\partial_x)$. A calculation shows that M has the form

$$\partial_x^2 + \frac{32\lambda^2}{9(1-4\lambda^2x^2)^2} - \frac{3\lambda^2}{4(1-4\lambda^2x^2)}$$

Order three with a 1-reducible Galois group

Let $T^3 + pT + q \in k[T]$ denote an irreducible polynomial with Galois group S_3 . Then the differential equation $y''' + py' + qy = 0$ has as basis for the solutions $y_i := e^{\alpha_i x}$ where $\alpha_1, \alpha_2, \alpha_3$ are the three roots of the polynomial $T^3 + pT + q$. The only relation over the field $\bar{k}(x)$ satisfied by the y_i is $y_1 y_2 y_3 = 1$. The differential Galois group is therefore a maximal torus in $Sl(3, \bar{k})$ and there are precisely three solutions of the Riccati equation, namely $\alpha_1, \alpha_2, \alpha_3$. This shows that the inequality in Theorem 2.5.6 part 1 is sharp.

Remarks

In the two remaining cases part 2 and 3 of Theorem 2.5.6 we are unable to give explicit examples to show that the inequalities are sharp.

Chapter 3

Shidlovskii irreducibility

3.1 Introduction

In this paper the notions Siegel normality and Shidlovskii irreducibility will be discussed. Being Siegel normal and being Shidlovskii irreducible are interesting properties of systems of ordinary linear differential equations, which arise in transcendental number theory. The aim of this article is to show how these properties can be characterized in terms of D -modules and the standard representation of the differential Galois group and how these characterizations can be used to verify Siegel normality or Shidlovskii irreducibility in some concrete practical examples.

The notion Siegel normality has been studied by F. Beukers, W.D. Brownawell and G. Heckman. Their important paper [BBH88] was the main source of inspiration for the research concerning the notion Shidlovskii irreducibility which led to this paper. Some interesting remarks on the notion Shidlovskii irreducibility are made in Bertrands paper [Ber90].

The following theorem is a fundamental theorem in the branch of transcendental number theory, which has been developed by C.L. Siegel and A.B. Shidlovskii. The theorem was proved by the latter one in 1959 (see [Shi89], Chapter 3).

Theorem 3.1.1 *Consider the $n \times n$ system of linear differential equations*

$$(A) : \quad \frac{d}{dz} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

where $a_{ij} \in \mathbf{C}(z)$ for all i, j . Assume that:

1. $(f_1(z), \dots, f_n(z))^t$ is a solution of the system (A) .
2. The component functions $f_1(z), \dots, f_n(z)$ are all E -functions.
3. The component functions $f_1(z), \dots, f_n(z)$ are homogeneous algebraic independent over $\mathbf{C}(z)$.

4. ξ is a nonzero algebraic number and ξ is not a pole of one of the a_{ij} 's.

Then the numbers $f_1(\xi), \dots, f_n(\xi)$ are homogeneous algebraic independent over $\mathbf{Q}$.

There exists also a more quantitative version of this theorem, namely if one adds the assumption that system (A) is homogeneous algebraic Siegel normal or that system (A) is homogeneous algebraic Shidlovskii irreducible, then one may conclude that the numbers $f_1(\xi), \dots, f_n(\xi)$ are homogeneous algebraic independent with an effective measure of homogeneous algebraic independence. So this quantitative version of Shidlovskii's fundamental theorem motivates the study of Siegel's normality criterion and Shidlovskii's weaker irreducibility criterion.

The paper is organized in the following manner. In section 3.2 some notation will be fixed and some basic facts from D -modules and differential Galois theory will be recalled. Section 3.3 contains a summary of the results of Beukers, Brownawell and Heckman. In section 3.4 the results concerning the notion Shidlovskii irreducibility will be discussed. Some nice examples will be given in section 3.5.

Finally I wish to thank M. van der Put for his advice and interest. And I also would like to express my gratitude to F. Beukers, who called my attention to the book [Shi89] and gave me some ideas.

3.2 Preliminaries

Definition 3.2.1 A differential field (K, δ) is a field K equipped with a derivation $\delta : K \rightarrow K$. That is $\delta(a + b) = \delta a + \delta b$ and $\delta(ab) = \delta(a)b + a\delta(b)$. The field of constants of K is $C = C_K = \{c \in K \mid \delta c = 0\}$.

From now on we will assume that $\text{char } K = \text{char } C = 0$ and that C is algebraically closed. For the purposes mentioned in the introduction one should take $K = \mathbf{C}(z)$, $C = \mathbf{C}$ and $\delta = \frac{d}{dz}$.

Definition 3.2.2 Let $M \supseteq K$ and $L \supseteq K$ be differential fields. A field isomorphism $\phi : L \rightarrow M$ is a differential K -isomorphism, if $\phi(a) = a$ for all $a \in K$ and $\phi(\delta a) = \delta \phi(a)$ for all $a \in L$. If $M = L$ then ϕ is a differential K -automorphism.

Consider the system of linear differential equations (A) : $\delta \mathbf{y} = A\mathbf{y}$, where A is a $n \times n$ -matrix with coefficients in K .

Definition 3.2.3 Differential field (L, δ^L) is called a Picard-Vessiot extension of K associated with (A) if

1. $L \supseteq K$ and $\delta^L|_K = \delta$.
2. $C_L = C_K = C$.

3. (A) has n linear independent solutions over C in L^n .
4. L is minimal with respect to the conditions 1,2 and 3 or equivalently if $U = (u_{ij})_{i,j=1,\dots,n} \in L^{n \times n}$ is a fundamental matrix of the system (A) then $L = K(u_{11}, \dots, u_{nn})$.

Theorem 3.2.4 *For every system of linear differential equations (A) there exists a Picard-Vessiot extension L and this extension is unique up to differential K -isomorphism.*

Definition 3.2.5 *The differential Galois group $DGal(L/K)$ is the group consisting of all the differential K -automorphisms of L .*

If $U \in L^{n \times n}$ is a fundamental matrix of system (A) and $\sigma \in DGal(L/K)$, then it's obvious that also $\sigma(U)$ is a fundamental matrix of system (A) . Hence

$$\sigma(U) = \begin{pmatrix} \sigma(u_{11}) & \cdots & \sigma(u_{1n}) \\ \vdots & & \vdots \\ \sigma(u_{n1}) & \cdots & \sigma(u_{nn}) \end{pmatrix} = \begin{pmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & & \vdots \\ u_{n1} & \cdots & u_{nn} \end{pmatrix} \cdot T_\sigma,$$

where $T_\sigma \in Gl(n, C)$. So the elements of the differential Galois group act as C -linear maps on the space of solutions $V = \{c_1 \mathbf{u}_1 + \cdots + c_n \mathbf{u}_n \mid c_1, \dots, c_n \in C\}$. ($\mathbf{u}_i = (u_{1i}, \dots, u_{ni})^t \in L^n$). But even a stronger statement holds.

Theorem 3.2.6 *$DGal(L/K)$ is a linear algebraic group over the field of constants C and*

$$\dim_C DGal(L/K) = \deg tr_K L = \deg tr_K(u_{11}, \dots, u_{nn}).$$

(By $\deg tr$ we mean degree of transcendence.) Further the Galois correspondence is of importance.

Theorem 3.2.7 *Suppose $G = DGal(L/K)$. Then the following statements holds:*

1. $(\forall \sigma \in G : \sigma(a) = a) \Rightarrow a \in K$.
2. If H is an algebraic subgroup of G such that $K = \{a \in L \mid \forall \sigma \in H : \sigma(a) = a\}$ then $H = G$.
3. There is a 1-1 correspondence between algebraic subgroups H and differential subfields M .

$$H = DGal(L/M) \Leftrightarrow M = \{a \in L \mid \forall \sigma \in H : \sigma(a) = a\}.$$

4. Under this correspondence normal subgroups $H \subseteq G$ correspond to Picard-Vessiot extensions $M \supseteq K$ and vice versa. And then we have

$$DGal(M/K) = G/H.$$

The first proofs of the last two theorems and the existence and uniqueness up to differential K -isomorphism of the Picard-Vessiot extension were given by E.R. Kolchin. (See [Kol 73], and [Lev90].) For more information about differential Galois theory we refer to [Kap57] and [Sin89].

Let $D = K\langle\partial\rangle$ be a skew polynomial ring consisting of all expressions $\sum_{i=0}^k a_i \partial^i$ with $a_i \in K$ for $i = 1, \dots, n$. The multiplication in D is completely fixed by the relation $\partial a = a\partial + \delta a$ if $a \in K$. To a system of linear differential equations $(A) : \delta \mathbf{y} = A\mathbf{y}$ with $A \in K^{n \times n}$ we associate a left D -module $M = K^n$ (In the sequel we mean by D -module M a left D -module M with $\dim_K M < \infty$.) in the following manner. If $m \in M$ then we define

$$\left(\sum_{i=0}^k a_i \partial^i\right) \cdot m := \sum_{i=0}^k a_i (\delta - A)^i \cdot m.$$

Conversely it's possible to associate a system of linear differential equations to a D -module M with a fixed K -base $E = \{e_1, \dots, e_n\}$ in a natural way. Namely if $E = \{e_1, \dots, e_n\}$ is a K -base of D -module M then there exist $a_{ij} \in K$ such that $\partial e_i = -\sum_{j=1}^n a_{ij} e_j$ for $j = 1, \dots, n$. Let $A = (a_{ij})_{i,j=1,\dots,n}$. If $m = \sum_{i=1}^n m_i e_i \in M$ then $\partial(m) = \sum_{i=1}^n \delta(m_i) e_i - \sum_{i=1}^n \sum_{j=1}^n a_{ij} m_i e_j$. Hence

$$\begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \mapsto \begin{pmatrix} \delta(m_1) \\ \vdots \\ \delta(m_n) \end{pmatrix} - A \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

describes ∂ in coordinates. Now the system (A) corresponding to the matrix A is the system of linear differential equations associated to D -module M with fixed K -base E . Let $(\tilde{A})$ be a system of linear differential equations associated to the same D -module with an other fixed K -base $\tilde{E} = \{\tilde{e}_1, \dots, \tilde{e}_n\}$ and let $\tilde{A} \in K^{n \times n}$ be the corresponding matrix. Suppose $\tilde{e}_i = \sum_{j=1}^n t_{ij} e_j$ for $i = 1, \dots, n$, where $t_{ij} \in K$ for all i, j . Then the matrix $T = (t_{ij})_{i,j=1,\dots,n} \in K^{n \times n}$ is invertible and we have the following relation.

$$\tilde{A} = TAT^{-1} + \delta(T)T^{-1}.$$

The systems (A) and $(\tilde{A})$ corresponding to the matrices A and $\tilde{A}$ are defined to be equivalent if the above relation holds for a certain invertible matrix $T \in K^{n \times n}$. In that case if $U \in L^{n \times n}$ is a fundamental matrix of (A) then $TU \in L^{n \times n}$ is a fundamental matrix of the system $(\tilde{A})$. Now it's obvious that the solution spaces $V, \tilde{V}$ of the systems $(A), (\tilde{A})$ are equivalent as representation spaces of the differential Galois group $DGal(L/K)$. And it is also clear that two Picard-Vessiot extensions $L, \tilde{L}$ associated with two equivalent systems $(A), (\tilde{A})$ are differential

K -isomorphic. Hence it is allowed to write $DGal(M)$ instead of $DGal(L/K)$ if L is a Picard-Vessiot extension associated with D -module M .

Recapitulating, we can view systems of linear differential equations as D -modules with a fixed K -base and D -modules as an equivalence class of systems of linear differential equations. We have introduced D -modules, because we prefer to study some properties of systems of linear differential equations K -base independently.

Let $L = L_M$ be a Picard-Vessiot extension associated with the D -module M . Then $L \otimes_K M$ becomes a $L\langle\partial\rangle$ -module if we define $\partial(a \otimes m) = \delta^L(a) \otimes m + a \otimes \partial(m)$. Then $V = V_M = \ker(\partial, L \otimes_K M)$ is the vector space of solutions on which the differential Galois group $G = DGal(M) = DGal(L/K)$ faithfully acts. We note that $L \otimes_C V = L \otimes_K M$, because if the elements $v_1, \dots, v_n \in V$ are linear independent over C , then it is not difficult to demonstrate that they are also linear independent over L . The differential Galois group acts on $L_M \otimes_C V$ by $\sigma(a \otimes v) = \sigma(a) \otimes \sigma(v)$ if $\sigma \in G$. By taking the G -invariant elements of $L_M \otimes_C V$ we recover M , i.e. $M = (L_M \otimes_C V)^G$. Moreover there is a 1-1 correspondence between D -submodules $\tilde{M} \subseteq M$ and G -stable subspaces $\tilde{V} \subseteq V$.

$$\tilde{M} \longmapsto L \otimes_K \tilde{M} \longmapsto \ker(\partial, L \otimes_K \tilde{M}) = \tilde{V}_{\tilde{M}}$$

$$\tilde{V} \longmapsto L_{\tilde{M}} \otimes_C \tilde{V} \longmapsto (L_{\tilde{M}} \otimes_C \tilde{V})^G = \tilde{M}_{\tilde{V}}$$

Because of this correspondence it's possible to replace M , N , D -(sub)modules and K by V , W , G -stable (sub)spaces in the next definitions and lemma's of this section. We denote $M \simeq N$ if M and N are isomorphic as D -modules and $V \simeq W$ if V and W are equivalent as representation spaces of G .

Definition 3.2.8 *D -module M is simple if there is no D -submodule $\tilde{M}$ such that $\{0\} \subset \tilde{M} \subset M$.*

(In this paper we use the symbol $\subset$ exclusively to denote a strict inclusion.)

Definition 3.2.9 *D -module M is indecomposable if there exist no D -submodules M_1, M_2 such that $\{0\} \subset M_1, M_2 \subset M$ and $M = M_1 \oplus M_2$.*

The next two classical lemmas will be used in this paper. Sometimes even tacitly!

Lemma 3.2.10 *(Krull-Schmidt). Let M be a D -module, $M = \bigoplus_{i=1}^k M_i$ and $M = \bigoplus_{j=1}^l \tilde{M}_j$, where the M_i and the $\tilde{M}_j$ are nontrivial indecomposable D -submodules. Then $k = l$ and there is a permutation $\pi \in S_k$ such that $M_i \simeq \tilde{M}_{\pi(i)}$ for $i = 1, \dots, k$.*

If N, M are D -modules and $N \subset M$, then there exist a sequence of D -modules $N = N_0 \subset N_1 \subset \cdots \subset N_k = M$ such that N_i/N_{i-1} is a simple D -module for $i = 1, \dots, k$. Such a sequence is called a Jordan-Hölder sequence from N to M .

Lemma 3.2.11 (*Jordan-Hölder*). *Let M be a D -module and let $\{0\} = M_0 \subset M_1 \subset \cdots \subset M_k = M$ and $\{0\} = \tilde{M}_0 \subset \tilde{M}_1 \subset \cdots \subset \tilde{M}_l = M$ be Jordan-Hölder sequences. Then $l = k$ and there is a permutation $\pi \in S_k$ such that $M_i/M_{i-1} \simeq \tilde{M}_{\pi(i)}/\tilde{M}_{\pi(i)-1}$ for $i = 1, \dots, k$*

Definition 3.2.12 *Let $\{0\} = M_0 \subset M_1 \subset \cdots \subset M_k = M$ be a Jordan-Hölder sequence from $\{0\}$ to M and let S be a simple D -module then we define $\text{mult}_S M := \#\{i \in \{1, \dots, k\} \mid M_i/M_{i-1} \simeq S\}$.*

The correctness of this definition is an immediate consequence of the Jordan-Hölder lemma.

Suppose M is a D -module. Let M^* denote its dual space, that is the vector space consisting of all the K -linear maps $l : M \rightarrow K$. It is possible to give M^* a D -module structure. Define $(\partial^* l)(m) = \delta(l(m)) - l(\partial(m))$ for all $m \in M$ if $l \in M^*$.

Definition 3.2.13 *D -modules M and $\tilde{M}$ are cogredient if there exists a one dimensional D -module N such that $M \simeq N \otimes_K \tilde{M}$ and they are contragredient if there exists a one dimensional D -module N such that $M \simeq N \otimes_K \tilde{M}^*$.*

3.3 Siegel normality

This section contains a brief description of the results concerning Siegel normality in [BBH88].

The definition of the notion of Siegel normality is rather subtle. Consider the square matrix $A := (a_{ij})_{i,j=1,\dots,n} \in K^{n \times n}$. Sometimes the matrix $A = (a_{ij})_{i,j=1,\dots,n}$ splits into r submatrices

$$A_t = (a_{ij})_{i,j=1,\dots,n_t}, \quad t = 1, \dots, r, \quad n_1 + \cdots + n_r = n.$$

That is the square submatrices A_t are located along the main diagonal of A and all of the entries outside these submatrices are zero:

$$A = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_r \end{pmatrix}.$$

We denote by (A) the system of differential equations which corresponds to the matrix A .

Definition 3.3.1 System (A) is called linear Siegel normal if for any solution $\mathbf{f} = (\mathbf{f}_1, \dots, \mathbf{f}_r)^t$ of (A), $\mathbf{f}_i = (f_{i1}, \dots, f_{in_i})^t$ and any $\mathbf{p}_i \in K^{n_i}$ the relation $\mathbf{p}_1 \mathbf{f}_1 + \dots + \mathbf{p}_r \mathbf{f}_r = 0$ implies for each $i = 1, \dots, r$ that either $\mathbf{p}_i = 0$ or $\mathbf{f}_i = 0$.

If $\mathbf{f} = (\mathbf{f}_1, \dots, \mathbf{f}_r)^t$ is a solution of system (A) then we let $\mathbf{f}^{l_1, \dots, l_r}$ denote a $N_{l_1, \dots, l_r}$ -tuple consisting of all the $N_{l_1, \dots, l_r}$ monomials

$$f_{11}^{j_{11}} \dots f_{1n_1}^{j_{1n_1}} f_{21}^{j_{21}} \dots f_{2n_2}^{j_{2n_2}} \dots f_{r1}^{j_{r1}} \dots f_{rn_r}^{j_{rn_r}}$$

in the component functions of the solution $\mathbf{f} = (\mathbf{f}_1, \dots, \mathbf{f}_r)^t$ with $\sum_{k=1}^{n_i} j_{ik} = l_i$ for $i = 1, \dots, r$. (The order of components in this $N_{l_1, \dots, l_r}$ -tuple doesn't matter.)

Definition 3.3.2 System (A) is called homogeneous algebraic Siegel normal if for any $N \geq 1$ and any solution $\mathbf{f} = (\mathbf{f}_1, \dots, \mathbf{f}_r)^t$ of (A) and any $\mathbf{p}_{l_1, \dots, l_r} \in K^{N_{l_1, \dots, l_r}}$

$$\sum_{l_1 + \dots + l_r = N} \mathbf{p}_{l_1, \dots, l_r} \mathbf{f}^{l_1, \dots, l_r} = 0$$

implies for all r -tuples $l_1, \dots, l_r$ with $l_1 + \dots + l_r = N$ that either $\mathbf{p}_{l_1, \dots, l_r} = 0$ or $\mathbf{f}^{l_1, \dots, l_r} = 0$.

These definitions can be translated easily into terms of D -modules.

Definition 3.3.3 Let $E = \{e_1, \dots, e_n\}$ be a K -base of the D -module M . Say $M = \bigoplus_{i=1}^r M_i$, where the M_i are D -submodules with $M_i = \text{span}_K(E_i)$, $E_i \subset E$. We assume that r is taken as large as possible. Now M is called linear Siegel normal with respect to this K -base E if for all $v \in V = \ker(\delta, L \otimes_K M)$, say $v = \sum_{i=1}^r v_i \in V$ with $v_i \in L \otimes_K M_i$ for $i = 1, \dots, r$ and for all K -linear maps $l : M \rightarrow K$ extended as L -linear map $(L \otimes_K M) \rightarrow L$ (i.e. $l \in (L \otimes_K M^*)^G$) we have $l(v) = 0$ implies for all i : $v_i = 0$ or $l(E_i) = \{0\}$.

Definition 3.3.4 Let $E = \{e_1, \dots, e_n\}$ be a K -base of the D -module M . Then M is called homogeneous algebraic Siegel normal with respect to the K -base E if $S^t M$ (t -th symmetric tensor power) is linear Siegel normal with respect to the K -base $S^t E = \{e_1^{t_1} \otimes_s e_2^{t_2} \otimes_s \dots \otimes_s e_n^{t_n} \mid t_i \in \mathbf{N}_{\geq 0}, \sum_{i=1}^n t_i = t\}$ for each $t \geq 1$.

Unfortunately being Siegel normal is a property, which is not invariant under base transformations, therefore the following base independent definition is added.

Definition 3.3.5 D -module M is called linear (homogeneous algebraic resp.) Siegel normal if there exists a K -base E of M such that M is linear (homogeneous algebraic resp.) Siegel normal with respect to this K -base E .

Theorem 3.3.6 *Let M be a D -module. Then the following statements are equivalent:*

1. M is linear Siegel normal.
2. The D -submodules M_i are simple for $i = 1, \dots, r$ and $M_i \not\simeq M_j$ if $i \neq j$.
3. The G -stable subspaces $V_i = \ker(\partial, L \otimes_K M_i)$ are simple for $i = 1, \dots, r$ and $V_i \not\simeq V_j$ if $i \neq j$.

Proof. The equivalence $2 \Leftrightarrow 3$ is an immediate consequence of the 1-1 correspondence between D -submodules $\tilde{M} \subset M$ and G -stable subspaces $\tilde{V} \subset V$. A proof of $1 \Leftrightarrow 2$ will be given.

$1 \Rightarrow 2$. Suppose M_i is not simple, then there exists a D -submodule $\tilde{M}_i$ with $\{0\} \subset \tilde{M}_i \subset M_i$. Let l be a K -linear map $M \rightarrow K$ with $\tilde{M}_i = \ker(l)$. Extend l as L -linear map $L \otimes_K M \rightarrow L$. Let $\tilde{V}_i = \ker(\partial, L \otimes_K \tilde{M}_i)$ and let $\tilde{v}_i \in \tilde{V}_i \setminus \{0\}$. Then one has $l(\tilde{v}_i) = 0$, $\tilde{v}_i \neq 0$ and $l(M_i) \neq 0$. Hence M is not linear Siegel normal if M_i is not simple.

Suppose $M_i \simeq M_j$. Then there exists a K -linear map $\phi: M_i \rightarrow M_j$ such that $\forall q \in D: \phi(q.m_i) = q.\phi(m_i)$. Extend ϕ as L -linear map $L \otimes_K M_i \rightarrow L \otimes_K M_j$. Let l_i be a K -linear map $M \rightarrow K$ extended as L -linear map $L \otimes_K M \rightarrow L$ such that $l_i(M_k) = \{0\}$ if $k \neq i$ and $l_i(v_i) \neq 0$ for a $v_i \in V_i$. Let $v_j = \phi(v_i)$. Define $l_j = l_i \circ \phi$ and $l = l_i - l_j$. Then $l(v_i + v_j) = 0$, $v_i \neq 0$, $v_j \neq 0$, $l(M_i) \neq \{0\}$ and $l(M_j) \neq \{0\}$. Hence M is not linear Siegel normal if $M_i \simeq M_j$ and $i \neq j$.

$2 \Rightarrow 1$. Let $l: M \rightarrow K$ be a K -linear map. Extend l as a L -linear map $(L \otimes_K M) = (L \otimes_C V) \rightarrow L$ and define $W = \{v \in V \mid l(v) = 0\}$. Clearly, W is a G -stable subspace of V . Consider also the corresponding D -submodule $N = (L \otimes_C W)^G$. $N = \bigoplus_{i \in I} M_i$ with $I \subseteq \{1, \dots, r\}$, because the D -modules M_i are simple for $i = 1, \dots, r$ and $M_i \not\simeq M_j$ if $i \neq j$. Of course $l(N) = \{0\}$ and also $l(M_i) = \{0\}$ for $i \in I$. Suppose $v \in V$, $v = \sum_{i=1}^r v_i$ with $v_i \in V_i = \ker(\delta, L \otimes_K M_i)$ for $i = 1, \dots, r$. If $l(v) = 0$ then we have $v_i = 0$ for $i \in \{1, \dots, k\} \setminus I$ and $l(M_i) = 0$ for $i \in I$. Hence M is linear Siegel normal if the M_i are simple and mutual non-equivalent. $\square$

The main results in [BBH88] are the next two theorems.

Theorem 3.3.7 *Let M be a D -module. Suppose $\dim_K M = n \geq 2$. Further let $G = D\text{Gal}(M)$. Then the following statements are equivalent:*

1. M is simple and homogeneous algebraic Siegel normal.
2. G contains $Sl(n, C)$ or $Sp(n, C)$

Theorem 3.3.8 *Let M be a D -module and let $G = D\text{Gal}(M)$. Then the following statements are equivalent:*

1. M is homogeneous algebraic Siegel normal.
2. $M = (\bigoplus_{i=1}^r M_i) \oplus (\bigoplus_{j=1}^s N_j)$, where the M_i are non-cogredient and non-contragredient simple linear Siegel normal D -modules with $\dim_K M_i \geq 2$ and the N_j are one dimensional D -modules satisfying the following condition:

$$S^{k_1} N_1 \otimes \cdots \otimes S^{k_s} N_s \simeq N_{triv}$$

implies either $k_1, \dots, k_s = 0$ or $\sum_{i=1}^s k_i \neq 0$. (Here N_{triv} denotes the trivial D -module, i.e. $N = Ke$ with $\partial e = 0$, and if $k \in \mathbf{Z}_{\leq -1}$ then $S^k N$ denotes the D -module $S^{-k} N^*$.)

3.4 Shidlovskii irreducibility

Consider the $n \times n$ system of linear differential equations

$$(A) : \quad \frac{d}{dz} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

where $a_{ij} \in K$ for all i, j .

Definition 3.4.1 System (A) is called linear Shidlovskii irreducible if for any solution $\mathbf{f} = (f_1, \dots, f_n)^t$ of (A) and any $p_i \in K$ the relation $p_1 f_1 + \cdots + p_n f_n = 0$ implies for each $i = 1, \dots, n$ that either $p_i = 0$ or $f_i = 0$. In other words system (A) is linear Shidlovskii irreducible if the nonzero components of every solution $\mathbf{f} = (f_1, \dots, f_n)^t$ are linear independent over K .

Definition 3.4.2 System (A) is called homogeneous algebraic Shidlovskii irreducible if the nonzero components of any solution are homogeneous algebraic independent over K .

Compare these definitions of Shidlovskii irreducibility with the corresponding definitions of Siegel normality. It is immediately clear that being linear (homogeneous algebraic resp.) Shidlovskii irreducible is a weaker property of systems of linear differential equations than being linear (homogeneous algebraic resp.) Siegel normal.

Translating above definitions into terms of D -modules we get:

Definition 3.4.3 Let $E = \{e_1, \dots, e_n\}$ be a K -base of the D -module M . M is called linear Shidlovskii irreducible with respect to the K -base E if for all K -linear maps $l : M \rightarrow K$ extended as L -linear map $L \otimes_K M \rightarrow L$ (i.e. $l \in (L \otimes_K M^*)^G$) and all $v = \sum_{i=1}^n v_i e_i \in V = \ker(\partial, L \otimes_K M)$ we have $l(v) = 0 \Rightarrow \forall i : v_i = 0$ or $l(e_i) = 0$.

Definition 3.4.4 Let $E = \{e_1, \dots, e_n\}$ be a K -base of the D -module M . Then M is called *homogeneous algebraic Shidlovskii irreducible* with respect to the K -base E if $S^t M$ is linear Shidlovskii irreducible with respect to the K -base $S^t E$ for each $t \geq 1$.

And now the base independent definition:

Definition 3.4.5 M is called *linear (homogeneous algebraic resp.) Shidlovskii irreducible* if there exists a K -base E such that M is linear (homogeneous algebraic resp.) Shidlovskii irreducible with respect to this K -base E .

Theorem 3.4.6 Let M be a D -module. Equivalent statements are:

1. M is linear Shidlovskii irreducible.
2. M has a K -base $E = \{e_1, \dots, e_n\}$ such that for every D -submodule $N \subseteq M$ there exists a subset $E_N \subseteq E$ such that $N = \text{span}_K E_N$.
3. There are only finitely many D -submodules $N \subseteq M$.
4. V has a C -base $F = \{f_1, \dots, f_n\}$ such that for every G -stable subspace $W \subseteq V$ there exists a subset $F_W \subseteq F$ such that $W = \text{span}_C F_W$.
5. There are only finitely many G -stable subspaces $W \subseteq V$.

Proof. The equivalence $3 \Leftrightarrow 5$ can be proved easily by the 1-1 correspondence between D -submodules $\tilde{M} \subseteq M$ and G -stable subspaces $\tilde{V} \subseteq V$. The proofs of $2 \Leftrightarrow 3$ and $4 \Leftrightarrow 5$ are completely analogous. A proof of $1 \Leftrightarrow 2 \Leftrightarrow 3$ will be given.

$1 \Rightarrow 2$. Assume that D -module M is linear Shidlovskii irreducible with respect to the K -base $E = \{e_1, \dots, e_n\}$. Suppose further that $v = \sum_{i=1}^n v_i e_i \in V$ and $E(v) = \{e_i \in E \mid v_i \neq 0\}$. We associate to v a D -submodule $M(v)$ which is the smallest D -submodule of M such that $L \otimes_K M(v)$ contains v . We note that

$$M(v) = (L \otimes_C \text{span}_C(G.v))^G$$

Consider a K -linear map $l : M \rightarrow K$ extended as L -linear map $L \otimes_K M = L \otimes_C V \rightarrow L$. Clearly, $l(v) = 0 \Rightarrow l(L \otimes_C \text{span}_C(G.v)) = \{0\}$. So we get:

$$l(M(v)) = \{0\} \Leftrightarrow l(v) = 0 \Leftrightarrow \forall_{e_i \in E(v)} l(e_i) = 0 \Leftrightarrow l(\text{span}_K E(v)) = 0.$$

The second equivalence holds because M is linear Shidlovskii irreducible with respect to the K -base E . Hence $M(v) = \text{span}_K E(v)$ for all $v \in V$. Further if $N \subseteq M$ is a D -submodule then $N = M(v_1) + \dots + M(v_s)$ for certain $v_1, \dots, v_s \in V$. From this we get that $E = \{e_1, \dots, e_n\}$ is a K -base of M such that for each D -submodule N we have $N = \text{span}_K E_N$ for a subset $E_N \subseteq E$.

$2 \Rightarrow 1$. We assume that $E = \{e_1, \dots, e_n\}$ is a K -base of M which satisfies the property of statement 2. For each $v \in V$ let $M(v) = (L \otimes_C \text{span}_C(G.v))^G$. By assumption there exists a subset $E(v) \subseteq E$ such that $M(v) = \text{span}_K E(v)$. If $v = \sum_{i=1}^n v_i e_i$ then $\forall i : e_i \in E \setminus E(v) \Rightarrow v_i = 0$ and if l is a K -linear map $l : M \rightarrow K$ extended as L -linear map $L \otimes_K M \rightarrow L$ then we have

$$l(v) = 0 \Rightarrow l(M(v)) = 0 \Rightarrow l(e_i) = 0 \text{ if } e_i \in E(v).$$

Hence M is linear Shidlovskii irreducible.

$2 \Rightarrow 3$. Trivial.

$3 \Rightarrow 2$. Define $\mathcal{N} = \{N \mid N \subseteq M \text{ is a } D\text{-submodule}\}$. Successively will be proved:

- A. For any $N, \tilde{N}, Q \in \mathcal{N}$ with $N \supseteq Q$ and $\tilde{N} \supseteq Q$ we have: $N = \tilde{N}$ if and only if $\text{mult}_S(N/Q) = \text{mult}_S(\tilde{N}/Q)$ for all simple D -modules S .
- B. $(\mathcal{N}, +, \cap)$ is a finite distributive lattice.
- C. There exists a K -base $E = \{e_1, \dots, e_n\}$ of M such that for all $N \in \mathcal{N}$ we have $N = \text{span}_K E_N$, where $E_N \subseteq E$.

A. $(\Rightarrow)$ Trivial. $(\Leftarrow)$ We will prove this by induction with respect to the length k of the Jordan-Hölder sequence from Q to N . If $k = 0$ there is nothing left to prove. Assume the statement holds for $k = l - 1$. Let $Q = N_0 \subset N_1 \subset \dots \subset N_l = N$ and $Q = \tilde{N}_0 \subset \tilde{N}_1 \subset \dots \subset \tilde{N}_l = \tilde{N}$ be two Jordan-Hölder sequences from Q to N respectively from Q to $\tilde{N}$. Let q be minimal with respect to the condition that $\tilde{N}_q/\tilde{N}_{q-1} \simeq N_1/N_0$. The existence of such a q is evident because $\text{mult}_{N_1/N_0}(\tilde{N}/Q) = \text{mult}_{N_1/N_0}(N/Q) \geq 1$. From the Jordan-Hölder lemma we get $\tilde{N}_{q-1} + N_1 \supset \tilde{N}_{q-1}$, because $\text{mult}_{N_1/N_0}(\tilde{N}_{q-1}/Q) = 0 < 1 = \text{mult}_{N_1/N_0}((\tilde{N}_{q-1} + N_1)/Q)$. So $\tilde{N}_{q-1} + N_1 = \tilde{N}_q$ because the finiteness of the number of submodules of M implies that any quotient of M cannot contain two copies of the same submodule. Hence $N \supseteq N_1, \tilde{N} \supseteq N_1$ and for all simple D -modules we have $\text{mult}_S(N/N_1) = \text{mult}_S(\tilde{N}/N_1)$. Now we can apply the induction hypothesis and conclude $N = \tilde{N}$.

B. We have to prove the distributivity of the lattice $\mathcal{N}$. First we will prove

$$\text{mult}_S(N + \tilde{N}) = \max(\text{mult}_S N, \text{mult}_S \tilde{N})$$

if S is a simple D -module and $N, \tilde{N} \in \mathcal{N}$. We will prove $\text{mult}_S(N + \tilde{N}) = \max(\text{mult}_S N, \text{mult}_S \tilde{N})$ by induction with respect to the length h of the Jordan-Hölder sequences from $\{0\}$ to N . If $h = 0$ everything is clear. Assume the statement holds for $h = k - 1$. Let $\{0\} = N_0 \subset N_1 \subset \dots \subset N_k = N$ be a Jordan-Hölder sequence from $\{0\}$ to N . As a consequence of the proof of

statement A) we have $N_1 \subseteq \tilde{N}$ if $\text{mult}_{N_1} \tilde{N} \geq 1$. Hence

$$\begin{aligned}
& \text{mult}_S(N + \tilde{N}) \\
&= \text{mult}_S(N + (\tilde{N} + N_1)) \\
&= \text{mult}_S(N/N_1 + (\tilde{N} + N_1)/N_1) + \delta_{SN_1} \\
&= \max(\text{mult}_S N/N_1, \text{mult}_S(\tilde{N} + N_1)/N_1) + \delta_{SN_1} \\
&= \max(\text{mult}_S N, \text{mult}_S(\tilde{N} + N_1)) \\
&= \max(\text{mult}_{N_1} N, \text{mult}_{N_1} \tilde{N}),
\end{aligned}$$

where $\delta_{SN_1} = 0$ if $S \not\simeq N_1$ and $\delta_{SN_1} = 1$ if $S \simeq N_1$.

The proof of $\text{mult}_S(N \cap \tilde{N}) = \min(\text{mult}_S N, \text{mult}_S \tilde{N})$ for each simple D -module S and any $N, \tilde{N} \in \mathcal{N}$ is dual analogous. (In that case Jordan-Hölder sequences from N to M and from $\tilde{N}$ to M have to be considered.)

Let $N, \tilde{N}, \hat{N} \in \mathcal{N}$. Then we have for each simple D -module S

$$\begin{aligned}
& \text{mult}_S N \cap (\tilde{N} + \hat{N}) \\
&= \min(\text{mult}_S N, \text{mult}_S(\tilde{N} + \hat{N})) \\
&= \min(\text{mult}_S N, \max(\text{mult}_S \tilde{N}, \text{ord}_S \hat{N})) \\
&= \max(\min(\text{mult}_S N, \text{mult}_S \tilde{N}), \min(\text{mult}_S N, \text{mult}_S \hat{N})) \\
&= \max(\text{mult}_S(N \cap \tilde{N}), \text{mult}_S(N \cap \hat{N})) \\
&= \text{mult}_S((N \cap \tilde{N}) + (N \cap \hat{N}))
\end{aligned}$$

Now we get as a consequence from A) that $\forall N, \tilde{N}, \hat{N} \in \mathcal{N} : N \cap (\tilde{N} + \hat{N}) = (N \cap \tilde{N}) + (N \cap \hat{N})$. In the same way it is possible to demonstrate that $\forall N, \tilde{N}, \hat{N} \in \mathcal{N} : N + (\tilde{N} \cap \hat{N}) = (N + \tilde{N}) \cap (N + \hat{N})$. Hence $(\mathcal{N}, +, \cap)$ is a finite distributive lattice.

C. Suppose $\mathcal{N} = \{M_0, M_1, \dots, M_s\}$ where $M_i \subset M_j \Rightarrow i < j$. Thus in particular $M_0 = \{0\}$ and $M_s = M$. For any $i \in \{0, \dots, s\}$ a set E_i satisfying the next two conditions will be constructed.

- i. E_i is a K -base of D -module $\sum_{j=0}^i M_j$.
- ii. $\forall j \in \{0, \dots, i\} : M_j := \text{span}_K(E_{M_j})$ with $E_{M_j} \subseteq E_i$.

Define $E_0 := \emptyset$. Of course E_0 satisfies the above conditions. Suppose $i \geq 1$. Now we assume that for all $j \in \{0, \dots, i-1\}$ a set E_j satisfying the conditions i) and ii) has been constructed. If $M_i = M_k + M_l$ with $0 < k, l < i$, then define $E_i := E_{i-1}$. Obviously, E_i satisfies the conditions i) and ii) if E_{i-1} satisfies these conditions. If $M_i \neq M_l + M_k$ for all k, l with $0 < k, l < i$, then there exists a unique $h \in \{0, \dots, i\}$ such that $M_h \subset M_i$ and M_i/M_h is a simple D -module. Suppose that $E_{M_i} = E_{M_h} \cup \tilde{E}_i$ (disjunct union) is a K -base of M_i , where $E_{M_h} \subseteq E_{i-1}$ is a K -base of M_h . Define $E_i := E_{i-1} \cup \tilde{E}_i$. Of course E_i satisfies condition ii). Now

we assume that E_i doesn't satisfy condition i) and derive a contradiction. In any case we have $\text{span}_K E_i = \sum_{j=0}^i M_j$. If the elements of E_i satisfy a linear dependence relation over K then there must be a $m \in (\text{span}_K E_{i-1} \cap \text{span}_K \tilde{E}_i) \setminus \{0\}$. In other words $0 \neq m \in (\sum_{j=0}^{i-1} M_j) \cap M_i$. But $m \notin \text{span}_K E_{M_h} \cap \text{span}_K \tilde{E}_i$. So $M_h \subset (\sum_{j=0}^{i-1} M_j) \cap M_i$. If $\sum_{j=0}^{i-1} (M_j \cap M_i) = M_i$ then $\sum_{j=0}^{i-1} M_j \supset M_i$ and so there exists $k, l : 0 < k < l < i$ such that $M_i = M_k + M_l$ (It is possible to choose M_k and M_l in such a way that M_i/M_k and M_i/M_l are simple D -modules.), but this is contradictory to an earlier assumption. Summarizing: if condition i) is not fulfilled then we have

$$M_h \subset (\sum_{j=0}^{i-1} M_j) \cap M_i = (\text{distributivity!}) \sum_{j=0}^{i-1} (M_j \cap M_i) \subset M_i,$$

contradicting that M_i/M_h is a simple D -module. Now we have obtained the desired contradiction and thus E_i satisfies condition i). We conclude that it is possible to construct successively sets E_i satisfying conditions i) and ii). Hence the set $E = E_s$ constructed this way is a K -base of M , which has the required property that $\forall N \in \mathcal{N} : N = \text{span}_K E_N$ with $E_N \subseteq E$. This finishes the proof of the theorem. $\square$

Theorem 3.4.7 *Let M be a D -module. Equivalent statements are:*

1. M is homogeneous algebraic Shidlovskii irreducible.
2. M has a K -base $E = \{e_1, \dots, e_n\}$ such that for all $t \geq 1$ and for each D -module $N \subseteq S^t M$ there exists a subset $E_N \subseteq S^t E$ such that $N = \text{span}_K E_N$.
3. The vector space of solutions V has a C -base $F = \{f_1, \dots, f_n\}$ such that for all $t \geq 1$ and for each G -stable subspace $W \subseteq S^t V$ there exists a subset $F_W \subseteq S^t F$ such that $W = \text{span}_C F_W$.

Theorem 3.4.8 *Let $E = \{e_1, \dots, e_n\}$ be a K -base of D -module M . Let $l_1, \dots, l_n$ be K -linear maps $M \rightarrow K$, extended as L -linear maps $L \otimes_K M \rightarrow L$, such that $l_i(e_j) = \delta_{ij}$ for $i, j = 1, \dots, n$. Then we have:*

1. The following statements are equivalent:
 - (a) M is linear Shidlovskii irreducible with respect to the K -base E .
 - (b) The vector space of solutions V has a C -base $F = \{f_1, \dots, f_n\}$ such that:
 - i. for every G -stable subspace $W \subseteq V$ there exists a subset $F_W \subseteq F$ such that $W = \text{span}_C(F_W)$.

- ii. for every G -stable subspace $W \subseteq V$, we have $f_i \in W, f_j \notin W \Rightarrow l_j(f_i) = 0$.

2. The following statements are equivalent:

- (a) M is homogeneous algebraic Shidlovskii irreducible with respect to the K -base E .
- (b) The vector space of solutions V has a C -base $F = \{f_1, \dots, f_n\}$ such that:
- i. for all $t \geq 1$ for every G -stable subspace $W \subseteq S^t V$ there exists a subset $F_W \subseteq S^t F$ such that $W = \text{span}_C(F_W)$.
- ii. for every G -stable subspace $W \subseteq V$, we have $f_i \in W, f_j \notin W \Rightarrow l_j(f_i) = 0$.

Proof. We will prove only statement 1. (a) $\Rightarrow$ (b). Because of the 1-1 correspondence between G -stable subspaces $W \subset V$ and D -modules $N \subset M$ we can choose and number $f_1, f_2, \dots, f_n$ in such a way that together with condition i) the following condition is satisfied: $\forall I \subset \{1, \dots, n\} : \text{span}_K\{e_i\}_{i \in I} \subset M$ is a D -module $\Leftrightarrow \text{span}_C\{f_i\}_{i \in I}$ is a G -stable subspace. Let $W \subset V$ be a G -stable subspace, then there exists a D -module N such that $W = \ker(\partial, L \otimes_K N)$. Suppose $N = \text{span}_K\{e_i\}_{i \in I}$ with $I \subset \{1, \dots, n\}$. Then $W = \text{span}_C\{f_i\}_{i \in I}$. If $j \notin I$ then $l_j(N) = 0$ and thus also $l_j(L \otimes_K N) = 0$ and $l_j(W) = 0$. From this we get $l_j(f_i) = 0$ if $i \in I$ and $j \notin I$.

(b) $\Rightarrow$ (a). We assume that V has a C -base $F = \{f_1, \dots, f_n\}$, which satisfies the conditions i) and ii). Let $v \in V$ and suppose that $\text{span}_C(G.v) = \text{span}_C\{f_i\}_{i \in I_v}$. Let l be a K -linear map $M \rightarrow K$, extended as L -linear map $L \otimes_K M \rightarrow L$ such that $l(v) = 0$. From ii) we get $l_j(v) = 0$ if $j \notin I_v$. Consider $M(v) = (L \otimes_C \text{span}_C(G.v))^G$. $M(v)$ is $\#I_v$ -dimensional and $l_j(M(v)) = 0$ if $j \notin I_v$. So $M(v) = \text{span}_K\{e_i\}_{i \in I_v}$ and $l(M(v)) = 0 \Rightarrow l(e_i) = 0$ for $i \in I_v$. We conclude that M is linear Shidlovskii irreducible with respect to the K -base $E = \{e_1, \dots, e_n\}$, because $l_j(v) = 0$ if $j \notin I_v$ and $l(e_i) = 0$ if $i \in I_v$. $\square$

It is possible to formulate a theorem analogous to theorem 3.4.8 for Siegel normality.

Theorem 3.4.9 *Let M be a D -module and let $\{0\} = M_0 \subset M_1 \subset \dots \subset M_r = M$ be a Jordan-Hölder sequence. Then we have:*

1. $\bigoplus_{i=1}^r M_i/M_{i-1}$ is linear Siegel normal $\Rightarrow M$ is linear Shidlovskii irreducible.
2. $\bigoplus_{i=1}^r M_i/M_{i-1}$ is homogeneous algebraic Siegel normal $\Rightarrow M$ is homogeneous algebraic Shidlovskii irreducible.

Proof. 1. Suppose M is not linear Shidlovskii irreducible then it is not difficult to show that there exist a quotient of M which contains two copies of the same simple submodule. Hence the graded module $\bigoplus_{i=1}^r M_i/M_{i-1}$ must contain two copies of the same simple submodule. But then $\bigoplus_{i=1}^r M_i/M_{i-1}$ is not linear Siegel normal because of theorem 3.3.6.

2. Suppose $\bigoplus_{i=1}^r M_i/M_{i-1}$ is homogeneous algebraic Siegel normal. Let $t_i \in \mathbf{N}$ for $i = 1, \dots, r$. Then according to lemma 2.1 in [BBH88] D -module $S_{t_1, \dots, t_r} = S^{t_1}(M_1/M_0) \otimes \dots \otimes S^{t_r}(M_r/M_{r-1})$ is simple and further $S_{t_1, \dots, t_r} \not\cong S_{\tilde{t}_1, \dots, \tilde{t}_r}$ if $\sum_{i=1}^r t_i = \sum_{i=1}^r \tilde{t}_i$ and $(t_1, \dots, t_r) \neq (\tilde{t}_1, \dots, \tilde{t}_r)$. Obviously if S is a simple D -module then $\text{mult}_S S^t(\bigoplus_{i=1}^r M_i/M_{i-1}) = \text{mult}_S S^t M$ for all $t \in \mathbf{Z}_{\geq 0}$. Hence $S^t M$ is homogeneous algebraic Shidlovskii irreducible because $S^t(\bigoplus_{i=1}^r M_i/M_{i-1}) = \bigoplus_{\sum t_i = t} S_{t_1, \dots, t_r}$. $\square$

We wish to remark that the converse of this theorem does not hold. For instance consider the $\mathbf{C}(z)\langle \partial \rangle$ -module $M = \mathbf{C}(z)e_1 + \mathbf{C}(z)e_2$, with $\partial e_1 = 0$ and $\partial e_2 = \frac{1}{z}e_1$ and its submodule $M_1 = \mathbf{C}(z)e_1$. It is not difficult to verify that M is linear and homogeneous algebraic Shidlovskii irreducible, but $M_1 \oplus M/M_1$ is neither linear nor homogeneous algebraic Siegel normal.

3.5 Examples

In this section the results of the previous sections will be applied to get some concrete examples of systems of linear differential equations which are homogeneous algebraic Shidlovskii irreducible but which are not homogeneous algebraic Siegel normal. We restrict ourselves to systems of linear differential equations on which Shidlovskii's fundamental theorem is applicable (See section 1).

Let $0 \leq p < q$, $\mu_1, \dots, \mu_p \in \mathbf{C}$ and $\lambda_1, \dots, \lambda_q \in \mathbf{C} \setminus \mathbf{Z}_{\leq 0}$. Then we define the generalized hypergeometric function

$$\phi_{\mu_1, \dots, \mu_p; \lambda_1, \dots, \lambda_q}(z) = \sum_{n=0}^{\infty} \frac{(\mu_1)_n \cdots (\mu_p)_n}{(\lambda_1)_n \cdots (\lambda_q)_n} \left(\frac{z}{q-p}\right)^{(q-p)n},$$

where $(\alpha)_0 = 1$ and $(\alpha)_n = \alpha(\alpha+1) \cdots (\alpha+n-1)$. The function $\phi_{\mu_1, \dots, \mu_p; \lambda_1, \dots, \lambda_q}$ satisfies the q -th order differential equation

$$(\dagger) \quad \left(\prod_{i=1}^q (\theta + r(\lambda_i - 1)) - z^r \prod_{i=1}^p (\theta + r\mu_i) \right) y = r^q (\lambda_1 - 1) \cdots (\lambda_q - 1),$$

where $r = q - p$ and $\theta = z \frac{d}{dz}$. (See [Shi89], chapter 5, §1.) If $\mu_1, \dots, \mu_p \in \mathbf{Q}$ and $\lambda_1, \dots, \lambda_q \in \mathbf{Q} \setminus \mathbf{Z}_{\leq 0}$ then $\phi_{\mu_1, \dots, \mu_p; \lambda_1, \dots, \lambda_q}$ is an E -function

First we consider the special case $p = 0$ and $q = 1$. Suppose $\lambda \in \mathbf{C} \setminus \mathbf{Z}_{\leq 0}$ then $\phi_\lambda(z) = \sum_{n=0}^{\infty} \frac{1}{(\lambda)_n} z^n$ satisfies the linear differential equation

$$y' = \frac{z+1-\lambda}{z}y + \frac{\lambda-1}{z} \quad (' = \frac{d}{dz}).$$

Theorem 3.5.1 *Let $\lambda \in \mathbf{Q} \setminus \mathbf{Z}_{\leq 0}$. Suppose ξ is a nonzero algebraic number. Then $\phi_\lambda(\xi)$ is a transcendental number with an effective measure of transcendence.*

Proof. Consider the system of linear differential equations

$$(\hat{A}) : \quad \frac{d}{dz} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \frac{z+1-\lambda}{z} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

Let $\psi_\lambda(z) = z^{1-\lambda}e^z$. Then $\hat{U} = \begin{pmatrix} \psi_\lambda & 0 \\ 0 & 1 \end{pmatrix}$ is a fundamental matrix of the system $(\hat{A})$. Let $L = \mathbf{C}(z)(\psi_\lambda)$. Then L is a Picard-Vessiot extension of $\mathbf{C}(z)$ associated with the system $(\hat{A})$. If $\sigma \in D\text{Gal}(L/\mathbf{C}(z))$ then $\sigma(\hat{U}) = \hat{U} \cdot \begin{pmatrix} \chi(\sigma) & 0 \\ 0 & 1 \end{pmatrix}$ where χ is a character of the differential Galois group. For all $m \geq 1$ we have $\chi^m \neq 1$ because $\psi_\lambda^m \notin \mathbf{C}(z)$. Hence the system $(\hat{A})$ is homogeneous algebraic Siegel normal as a consequence of theorem 3.3.8 and so the system of linear differential equations

$$(\tilde{A}) : \quad \frac{d}{dz} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \frac{z+1-\lambda}{z} & \frac{\lambda-1}{z} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

is homogeneous algebraic Shidlovskii irreducible because of theorem 3.4.9. Further $(\phi_\lambda, 1)^t$ is a solution of the system $(\tilde{A})$ consisting of nonzero E -functions. Hence the numbers $\phi_\lambda(\xi), 1$ are homogeneous algebraic independent with an effective measure of homogeneous algebraic independence and so $\phi_\lambda(\xi)$ is transcendental with an effective measure of transcendence. $\square$

Theorem 3.5.2 *Let $\mu_1, \dots, \mu_p \in \mathbf{Q}$, $\lambda_1, \dots, \lambda_p \in \mathbf{Q} \setminus \mathbf{Z}$, $0 \leq p < q$. Suppose that $q \geq 2$ and that at least one of the following conditions holds.*

1. $\lambda_i - \mu_j \notin \mathbf{Z}$ for $1 \leq i \leq p$, $1 \leq j \leq q$ and the sums $\lambda_i + \lambda_j$ ($1 \leq i \leq j \leq q$) are all distinct modulo $\mathbf{Z}$.
2. $p = 0$, $q = 2$ or q is odd and there is not a permutation $\pi \in S_q$ and a divisor $d > 1$ of q such that $\lambda_i = \lambda_{\pi(i)} + \frac{1}{d} \pmod{\mathbf{Z}}$ for $i = 1, \dots, q$.

Let ξ be a nonzero algebraic number. Then the numbers

$$\phi_{\mu_1, \dots, \mu_p; \lambda_1, \dots, \lambda_q}(\xi), \dots, \phi_{\mu_1, \dots, \mu_p; \lambda_1, \dots, \lambda_q}^{(p-1)}(\xi)$$

are algebraic independent with an effective measure of algebraic independence.

Proof. Consider the homogeneous linear differential equation

$$\left(\prod_{i=1}^q (\theta + r(\lambda_i - 1)) - z^r \prod_{i=1}^p (\theta + r\mu_i) \right) y = 0$$

The $q \times q$ system corresponding to this differential equation is simple and homogeneous algebraic Siegel normal. For a proof of this statement we refer to proposition 4.4 and the proof of theorem 4.5 in [BBH88]. Hence the $(q+1) \times (q+1)$ system of differential equations corresponding to $(\dagger)$ is homogeneous algebraic Shidlovskii irreducible. And so the numbers

$$\phi_{\mu_1, \dots, \mu_p; \lambda_1, \dots, \lambda_q}(\xi), \dots, \phi_{\mu_1, \dots, \mu_p; \lambda_1, \dots, \lambda_q}^{(p-1)}(\xi)$$

are algebraic independent with an effective measure of algebraic independence. $\square$

Let $\lambda, \mu \in \mathbf{C} \setminus \mathbf{Z}_{\leq -1}$. Then we define the function

$$K_{\lambda, \mu}(z) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(\lambda+1)_n (\mu+1)_n} \left(\frac{z}{2}\right)^{2n},$$

which satisfies the non-homogeneous second order differential equation

$$y'' + \frac{2\lambda + 2\mu + 1}{z} y' + \left(1 + \frac{4\lambda\mu}{z^2}\right) y = \frac{4\lambda\mu}{z^2}$$

It is useful to define also the function $K_{\lambda, \mu; \xi}(z) = K_{\lambda, \mu}(\xi z)$, if $\lambda, \mu \in \mathbf{C} \setminus \mathbf{Z}_{\leq -1}$ and $\xi \in \mathbf{C}$. If $\lambda, \mu \in \mathbf{Q} \setminus \mathbf{Z}_{\leq -1}$ and ξ is an algebraic number then $K_{\lambda, \mu; \xi}$ is an E -function. (See [Shi89], chapter 5, §1.) The function $K_{\lambda, \mu; \xi}$ satisfies the equation

$$y'' + \frac{2\lambda + 2\mu + 1}{z} y' + \left(\xi^2 + \frac{4\lambda\mu}{z^2}\right) y = \frac{4\lambda\mu}{z^2}.$$

Lemma 3.5.3 *Consider the corresponding homogeneous differential equation*

$$(\dagger) \quad y'' + \frac{2\lambda + 2\mu + 1}{z} y' + \left(\xi^2 + \frac{4\lambda\mu}{z^2}\right) y = 0.$$

Let G be the differential Galois group over $\mathbf{C}(z)$ associated with this differential equation. If $\lambda - \mu + \frac{1}{2} \notin \mathbf{Z}$ and $\xi \neq 0$ then G contains $Sl(2, \mathbf{C})$.

Proof. Let $\overline{\mathbf{C}(z)}$ be the algebraic closure of $\mathbf{C}(z)$. We will prove that $\overline{G} = DGal((\dagger), \overline{\mathbf{C}(z)}) \simeq Sl(2, \mathbf{C})$. Hence G contains $Sl(2, \mathbf{C})$.

After transforming the differential equation by the substitution $x = z^{\lambda+\mu} y$ we get a new equation

$$(\ddagger) \quad x'' + \frac{1}{z} x' + \left(\xi^2 - \frac{(\lambda - \mu)^2}{x^2}\right) y = 0.$$

The differential equations $(\dagger)$ and $(\ddagger)$ are equivalent over $\overline{\mathbf{C}(z)}$. It is known that under the conditions of this lemma $DGal((\ddagger), \mathbf{C}(z)) \simeq Sl(2, \mathbf{C})$. (See [Kol68].) $Sl(2, \mathbf{C})$ is connected and $[DGal((\ddagger), \mathbf{C}(z)) : DGal((\dagger), \mathbf{C}(z))] < \infty$. Hence $DGal((\dagger), \overline{\mathbf{C}(z)}) \simeq Sl(2, \mathbf{C})$ and thus $\overline{G} \simeq Sl(2, \mathbf{C})$. $\square$

Let $A_{\lambda, \mu; \xi} = \begin{pmatrix} 0 & 1 \\ -\xi^2 - \frac{4\lambda\mu}{z^2} & \frac{-2\lambda-2\mu-1}{z} \end{pmatrix}$. Then the 2×2 system of linear differential equations $(A_{\lambda, \mu; \xi}) : y' = A_{\lambda, \mu; \xi} y$ is the system corresponding to the second order linear differential equation $(\dagger)$.

Lemma 3.5.4 *Consider the systems of linear differential equations $(A_{\lambda_1, \mu_1; \xi_1})$ and $(A_{\lambda_2, \mu_2; \xi_2})$. Suppose that $\lambda_i - \mu_i + \frac{1}{2} \notin \mathbf{Z}$, $i = 1, 2$ and $\xi_1, \xi_2 \neq 0$. Suppose further that the systems $(A_{\lambda_1, \mu_1; \xi_1})$ and $(A_{\lambda_2, \mu_2; \xi_2})$ are cogrediënt or contragrediënt. Then $\xi_1^2 = \xi_2^2$ and either $(\lambda_1 - \mu_1) + (\lambda_2 - \mu_2) \in \mathbf{Z}$ or $(\lambda_1 - \mu_1) - (\lambda_2 - \mu_2) \in \mathbf{Z}$.*

Proof. Let $U_1 = \begin{pmatrix} f_1 & g_1 \\ f'_1 & g'_1 \end{pmatrix}$ and $U_2 = \begin{pmatrix} f_2 & g_2 \\ f'_2 & g'_2 \end{pmatrix}$ be fundamental matrices of the systems $(A_{\lambda_1, \mu_1; \xi_1})$ and $(A_{\lambda_2, \mu_2; \xi_2})$. Then

$$3 \leq \deg \operatorname{tr}_{\mathbf{C}(z)}(f_1, f'_1, g_1, g'_1, f_2, f'_2, g_2, g'_2) \leq 4,$$

because the systems $(A_{\lambda_1, \mu_1; \xi_1})$ and $(A_{\lambda_2, \mu_2; \xi_2})$ are cogrediënt or contragrediënt and

$$\deg \operatorname{tr}_{\mathbf{C}(z)}(f_1, f'_1, g_1, g'_1) = \dim_{\mathbf{C}} DGal((A_{\lambda_1, \mu_1; \xi_1}), \mathbf{C}(z)) = 3.$$

Let $\tilde{f}_i = z^{\lambda_i + \mu_i} f_i$ and $\tilde{g}_i = z^{\lambda_i + \mu_i} g_i$, $i = 1, 2$ and let $V_i = \begin{pmatrix} \tilde{f}_i & \tilde{g}_i \\ \tilde{f}'_i & \tilde{g}'_i \end{pmatrix}$, $i = 1, 2$, then

$$V_i = M_i U_i, \text{ where } M_i = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ if } \lambda_i + \mu_i = 0 \text{ and else } M_i = \begin{pmatrix} z^{\lambda_i + \mu_i} & 0 \\ z^{\lambda_i + \mu_i - 1} & z^{\lambda_i + \mu_i} \end{pmatrix}.$$

It is easy to verify that V_i is a fundamental matrix of the system of differential equations $(B_i) : y' = \begin{pmatrix} 0 & 1 \\ -\xi_i^2 - \frac{(\lambda_i - \mu_i)^2}{z^2} & -\frac{1}{z} \end{pmatrix} y$. According to [Kol68]

$\deg \operatorname{tr}_{\mathbf{Q}(z)}(\tilde{f}_1, \tilde{f}'_1, \tilde{g}_1, \tilde{g}'_1, \tilde{f}_2, \tilde{f}'_2, \tilde{g}_2, \tilde{g}'_2) < 6$ implies $\xi_1^2 = \xi_2^2$ and either $(\lambda_1 - \mu_1) + (\lambda_2 - \mu_2) \in \mathbf{Z}$ or $(\lambda_1 - \mu_1) - (\lambda_2 - \mu_2) \in \mathbf{Z}$. $\square$

Theorem 3.5.5 *Suppose that $\lambda_i, \mu_i \in \mathbf{Q} \setminus \mathbf{Z}_{\leq -1}$, $i = 1, \dots, n$, $n \geq 1$, satisfy the conditions $\lambda_i - \mu_i + \frac{1}{2} \notin \mathbf{Z}$, and $(\lambda_{i_1} - \mu_{i_1}) + (\lambda_{i_2} - \mu_{i_2}) \notin \mathbf{Z}$, $(\lambda_{i_1} - \mu_{i_1}) - (\lambda_{i_2} - \mu_{i_2}) \notin \mathbf{Z}$, $i_1, i_2 = 1, \dots, n$, $i_1 \neq i_2$. Let $\xi_1, \dots, \xi_m$, $m \geq 1$, be nonzero algebraic numbers such that $\xi_i^2 \neq \xi_j^2$ if $i \neq j$. Then the $2mn$ numbers $K_{\lambda_i, \mu_i}(\xi_j), K'_{\lambda_i, \mu_i}(\xi_j)$, $i = 1, \dots, n$ $j = 1, \dots, m$, are algebraic independent with an effective measure of algebraic independence.*

Proof. Consider the $(2mn + 1) \times (2mn + 1)$ system of linear differential

equations

$$(\hat{A}) : y' = \begin{pmatrix} A_{\lambda_1, \mu_1; \xi_1} & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & & \vdots & \vdots \\ 0 & \cdots & A_{\lambda_i, \mu_i; \xi_j} & \cdots & 0 & 0 \\ \vdots & & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & A_{\lambda_n, \mu_n; \xi_m} & 0 \\ 0 & \cdots & 0 & \cdots & 0 & 0 \end{pmatrix} y.$$

System $(\hat{A})$ is homogeneous algebraic Siegel normal because of lemma 3.5.3, lemma 3.5.4 and theorem 3.3.8. Let $B_{i,j} = \begin{pmatrix} 0 \\ 4\lambda_i\mu_i \end{pmatrix}$ Then the system

$$(A) : y' = \begin{pmatrix} A_{\lambda_1, \mu_1; \xi_1} & \cdots & 0 & \cdots & 0 & B_{1,1} \\ \vdots & \ddots & \vdots & & \vdots & \vdots \\ 0 & \cdots & A_{\lambda_i, \mu_i; \xi_j} & \cdots & 0 & B_{i,j} \\ \vdots & & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & \cdots & A_{\lambda_n, \mu_n; \xi_m} & B_{n,m} \\ 0 & \cdots & 0 & \cdots & 0 & 0 \end{pmatrix} y$$

is homogeneous algebraic Shidlovskii irreducible because of theorem 3.4.9.

The $2mn + 1$ -tuple $(K_{\lambda_1, \mu_1; \xi_1}, \dots, K_{\lambda_i, \mu_i; \xi_j}, \dots, K_{\lambda_n, \mu_n; \xi_m}, 1)^t$ is a solution of the system (A) consisting of nonzero E -functions. Hence the numbers

$$K_{\lambda_1, \mu_1; \xi_1}(1), \dots, K_{\lambda_i, \mu_i; \xi_j}(1), \dots, K_{\lambda_n, \mu_n; \xi_m}(1), 1$$

are homogeneous algebraic independent with an effective measure of homogeneous algebraic independence and so the numbers

$$K_{\lambda_1, \mu_1}(\xi_1), \dots, K_{\lambda_i, \mu_i}(\xi_j), \dots, K_{\lambda_n, \mu_n}(\xi_m)$$

are algebraic independent with an effective measure of algebraic independence.

□

Chapter 4

An algorithm determining the difference Galois group of second order linear difference equations

4.1 Introduction

Let $K = k(z)$, where k is a finite algebraic extension of $\mathbf{Q}$ and z is a transcendental variable. Furthermore, let ϕ be the k -linear automorphism given by $\phi(z) = z + 1$. In this article we will describe an algorithm for determining the difference Galois group of the second order linear homogeneous difference equation $\phi^2 y + a\phi y + by = 0$ with $a, b \in K$. If the difference Galois group of an second order difference equation does not contain the group $Sl(2, \mathbf{Q})$ then one can compute two linear independent Liouvillian solutions in a sequence space for this equation. This will be explained in the section which is devoted to examples. This algorithm can be considered as an analogue for second order linear difference equations of Kovacic's algorithm for second order linear differential equations (See [Kov86]).

In [Pet92] an algorithm for finding rational solutions of the Riccati equation of arbitrary order is given. So the algorithm is not completely new. However the rationality result for solutions of the Riccati equation (Theorem 4.4.3) seems to be new.

In section 4.2 we summarize the results of [PS96] concerning difference Galois theory which are needed for our purposes. In section 4.3 we discuss first order homogeneous linear difference equations. The algorithm for determining the difference Galois group of second order homogeneous linear difference equations is described in section 4.4. Section 4.5 is devoted to examples.

4.2 Preliminaries on difference Galois theory

Let $\bar{\mathbf{Q}}$ denote the algebraic closure of $\mathbf{Q}$ and let $\hat{K} = \bar{\mathbf{Q}}(z)$. Let ϕ be the $\bar{\mathbf{Q}}$ -linear automorphism of $\hat{K}$ given by $\phi(z) = z + 1$. Consider the system of difference equations (A) : $\phi \mathbf{y} = A \mathbf{y}$, where $A \in Gl(n, \hat{K})$. (We restrict ourselves to equations with $A \in Gl(n, \hat{K})$ in order to guarantee that we get n independent solutions.)

Definition 4.2.1 *A ring R together with a fixed automorphism $\phi_R : R \rightarrow R$ is called a Picard-Vessiot extension of $\hat{K}$ associated with (A) if*

1. *R is a commutative ring, $R \supseteq \hat{K}$ and $\phi_R|_{\hat{K}} = \phi$.*
2. *The only ϕ_R -invariant ideals are 0 and R .*
3. *There exists a matrix $U \in Gl(n, R)$ such that $\phi_R(U) = AU$. (Such a matrix U is called a fundamental matrix for the system (A).)*
4. *R is minimal with respect to the conditions 1,2 and 3 or equivalently if $U = (u_{ij}) \in Gl(n, R)$ is a fundamental matrix for the system (A) then $R = \hat{K}[u_{11}, \dots, u_{nn}, \frac{1}{\det(U)}]$.*

Definition 4.2.2 *Consider the difference rings R_1 and R_2 together with their automorphisms ϕ_{R_1} and ϕ_{R_2} respectively. A ring homomorphism $\psi : R_1 \rightarrow R_2$ is called a difference-homomorphism if $\psi \phi_{R_1} = \phi_{R_2} \psi$.*

Theorem 4.2.3 *For every system of linear difference equations (A) there exists a Picard-Vessiot extension R and this extension is unique up to difference $\hat{K}$ -isomorphism. Furthermore, we have $\phi(r) = r$ implies $r \in \bar{\mathbf{Q}}$.*

From now on we will denote the extended automorphism ϕ_R of a Picard-Vessiot extension R also by ϕ .

Definition 4.2.4 *The difference Galois group $DGal(R/\hat{K})$ is the group consisting of all the difference $\hat{K}$ -automorphisms of R .*

If $U \in Gl(n, R)$ is a fundamental matrix of system (A) and $\sigma \in G = DGal(R/\hat{K})$, then it is obvious that also $\sigma(U)$ is a fundamental matrix of system (A). Hence

$$\sigma(U) = \begin{pmatrix} \sigma(u_{11}) & \cdots & \sigma(u_{1n}) \\ \vdots & & \vdots \\ \sigma(u_{n1}) & \cdots & \sigma(u_{nn}) \end{pmatrix} = \begin{pmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & & \vdots \\ u_{n1} & \cdots & u_{nn} \end{pmatrix} \cdot T_\sigma,$$

where $T_\sigma \in Gl(n, \bar{\mathbf{Q}})$. So the elements of the differential Galois group act as $\bar{\mathbf{Q}}$ -linear maps on the space of solutions $V = \{c_1 \mathbf{u}_1 + \cdots + c_n \mathbf{u}_n \mid c_1, \dots, c_n \in \bar{\mathbf{Q}}\}$. ($\mathbf{u}_i = (u_{1i}, \dots, u_{ni})^t \in R^n$). But even a stronger statement holds.

Theorem 4.2.5 $G = D\text{Gal}(R/\hat{K})$ is a linear algebraic group over the field of constants $\bar{\mathbf{Q}}$.

If G is an algebraic subgroup of $Gl(n, \bar{\mathbf{Q}})$, then we denote by $G(\hat{K})$ the subgroup of $Gl(n, \hat{K})$ which is defined by the same equations. That is $G(\hat{K})$ consists of the $\hat{K}$ -valued points of the algebraic group G .

Theorem 4.2.6 Suppose $G = D\text{Gal}(R/\hat{K})$. Then the following statements holds:

1. $(\forall \sigma \in G : \sigma(a) = a) \Rightarrow a \in \hat{K}$.
2. If H is an algebraic subgroup of G such that $\hat{K} = \{a \in R \mid \forall \sigma \in H : \sigma(a) = a\}$ then $H = G$.

Two systems (A) and (B) corresponding to matrices $A, B \in Gl(n, \hat{K})$ are defined to be equivalent if there exists a $T \in Gl(n, \hat{K})$ such that $B = \phi(T)AT^{-1}$. In this case if $U \in Gl(n, R)$ is a fundamental matrix of system (A) then TU is a fundamental matrix of system (B) and it is obvious that the solution spaces V_A, V_B of the systems (A) and (B) are equivalent as representation spaces of the difference Galois group. Conversely if the Picard-Vessiot extensions associated to the systems (A) and (B) are difference $\hat{K}$ -isomorphic and the solution spaces V_A and V_B are equivalent as representation spaces of the difference Galois group then (A) and (B) are equivalent systems of difference equations.

Theorem 4.2.7 Let $G \subseteq Gl(n, \bar{\mathbf{Q}})$ be the difference Galois group associated to the system of difference equations (A) . Let G^0 denote the identity component of G . Then the following statements hold.

1. G/G^0 is a finite cyclic group.
2. There exists a $B \in G(\hat{K})$ such that (A) and (B) are equivalent systems.

It is a conjecture that for every linear algebraic group $G \subseteq Gl(n, \bar{\mathbf{Q}})$ with G/G^0 finite cyclic there exists a system of difference equations which has G as difference Galois group. One can show that this conjecture is true for $n = 1, 2$ by giving explicit examples for every possible group.

Theorem 4.2.8 If $A \in G(\hat{K})$ with G an algebraic subgroup of $GL(n, \bar{\mathbf{Q}})$ such that for any proper algebraic subgroup H and for any $T \in G(\hat{K})$ one has that $\phi(T)AT^{-1} \notin H(\hat{K})$ then G is the difference Galois group of the system (A) .

If A satisfies the conditions of theorem above then we say that system (A) is in *standard form*. This standard form is in general not unique. But one can read off fairly easily the difference Galois group of a system of difference equations if one knows already that this system is in standard form. In fact we will present an

algorithm which computes for a given equation an equivalent system in standard form. The standard form is also very suitable for finding closed form solutions if the difference Galois group is not too big, that is does not contain the group $Sl(2, \bar{\mathbf{Q}})$.

We note that definitions and theorems 4.2.1 up to 4.2.6 could have been stated for (more) general difference rings. However theorems 4.2.7 and 4.2.8 are not valid for general difference rings. For the proofs and much more information about difference Galois theory we refer to [PS96].

4.3 First order difference equations

Let $K = k(z)$, where k is a finite algebraic extension of $\mathbf{Q}$. We consider the first order homogeneous linear difference equation (a) : $\phi y = ay$, where $a \in K^*$. Any equivalent equation is given by $\phi y = \frac{\phi(f)}{f} ay$, where $f \in \hat{K}^*$. The difference Galois group of (a) is a finite cyclic group of order n if there is an $f \in \hat{K}^*$ such that $\frac{\phi(f)}{f} a$ is a primitive n^{th} -root of unity, otherwise the difference Galois group is the multiplicative group $\mathbf{G}_m = \bar{\mathbf{Q}}^*$. This statement is a consequence of theorems 4.2.7 and 4.2.8.

Suppose $a \in K$ is given. We describe an algorithm which produces an element $b \in K$ such that the difference equations (a) and (b) : $\phi y = by$ are equivalent and $b = \frac{P}{Q}$ with $P, Q \in k[z]$ satisfying the condition that for all $m \in \mathbf{Z}$ we have $\gcd(P, \phi^m Q) = 1$. If b satisfies these conditions then we call b *reduced* and the difference equation (b) is automatically in standard form. The algorithm avoids factorization in $k[z]$.

We assume that $a = \frac{P}{Q}$ with $P, Q \in k[z]$ and $\gcd(P, Q) = 1$. There exists an $r > 0$ such that the zeros of P and Q are in the disk $|z| \leq r$. We can express r in terms of the coefficients of P and Q . For instance if $P = P_c z^c + \dots + P_1 z + P_0$ and $Q = Q_d z^d + \dots + Q_1 z + Q_0$ then we can take $r = [1 + \max(\sum_{i=0}^{c-1} |\frac{P_i}{P_c}|, \sum_{j=0}^{d-1} |\frac{Q_j}{Q_d}|)]$. For $m \in \mathbf{Z}$ with $|m| \geq 2r$ we have $\gcd(P, \phi^m Q) = 1$. We start with $m = 1$ and compute $g = \gcd(P, \phi(Q))$. If $g \neq 1$ then one can write $a = \frac{g}{\phi^{-1}(g)} \frac{\tilde{P}}{\tilde{Q}}$ and we can go further with $\tilde{a} = \frac{\tilde{P}}{\tilde{Q}}$ instead of a . This gives a reduction of the problem with respect to degrees of P and Q . If $g = 1$ then we try $m = -1$ and so forth. The algorithm stops if a is reduced to a constant or if all $m \in \mathbf{Z}$ with $|m| \leq 2r$ are checked off.

The above algorithm can easily be modified so that we also find an $f \in K$ that insures that $b = \frac{\phi(f)}{f} a$ is reduced.

For another approach using the resultant of $P(z)$ and $Q(z + m)$ we refer to [Pet92]. This approach works for more general fields.

4.4 Second order difference equations

Consider the second order linear homogeneous difference equation $\phi^2 y + a\phi y + by = 0$, where $a, b \in K$ and $b \neq 0$. As usual we will identify this equation with the 2×2 system of difference equations $(A) : \phi \mathbf{y} = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \mathbf{y}$. Throughout this section we will denote the difference Galois group of above system by G and the vector space of solutions on which G faithfully acts by V .

We present an algorithm which produces a matrix $B \in Gl(2, \hat{K})$ so that the systems (A) and (B) are equivalent and (B) is in standard form. Further a matrix T is computed such that $B = \phi(T)AT^{-1}$.

Lemma 4.4.1 *The algebraic subgroups G of $Gl(2, \bar{\mathbf{Q}})$ that can occur as difference Galois group are*

1. *Any reducible subgroup of $Gl(2, \bar{\mathbf{Q}})$ with G/G^0 finite cyclic.*
2. *Any infinite imprimitive subgroup of $Gl(2, \bar{\mathbf{Q}})$ with G/G^0 finite cyclic.*
3. *Any algebraic group containing $SL(2, \bar{\mathbf{Q}})$.*

Proof. This is a consequence of theorem 4.2.7 part 1 and the well known classification of the algebraic subgroups of $Gl(2, \bar{\mathbf{Q}})$.

The algorithm is arranged in the following manner. Given a second order difference equation we test which of the three cases above holds. After that we compute an appropriate equivalent system in standard form.

4.4.1 The Riccati equation

To a second order linear difference equation $\phi^2 y + a\phi y + by = 0$, where $a, b \in K$ and $b \neq 0$ we can associate a first order non-linear difference equation $(\dagger) : u\phi(u) + au + b = 0$. This equation is called the Riccati equation. If u is a solution of the Riccati equation then the difference operator $\phi^2 + a\phi + b$ factors as $(\phi - \frac{b}{u})(\phi - u)$. A rational solution of the Riccati equation corresponds to a line in the solutionspace that is fixed by the difference Galois group. Therefore we have the following theorem.

Theorem 4.4.2 *The following statements hold:*

1. *If the Riccati equation has no solutions $u \in \hat{K}^*$ then G is irreducible.*
2. *If the Riccati equation has exactly one solution $u \in \hat{K}^*$ then G is reducible but not completely reducible.*
3. *If the Riccati equation has exactly two solutions $u_1, u_2 \in \hat{K}^*$ then G is completely reducible but G is not an algebraic subgroup of $\{c.Id \mid c \in \bar{\mathbf{Q}}^*\}$.*

4. If the Riccati equation has more than two solutions in $\hat{K}^*$ then the Riccati equation has infinitely many solutions and G is an algebraic subgroup of $\{c.Id \mid c \in \bar{\mathbf{Q}}^*\}$.

Proof. We can prove this theorem can very directly using theorems 4.2.7 and 4.2.8.

1. If G is reducible then according to theorem 4.2.7 there exists an upper triangular matrix $B \in Gl(2, \bar{K})$ and a matrix $T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \in Gl(2, \hat{K})$ such that $B = \phi(T) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T^{-1}$. One can easily verify that $t_{22} \neq 0$ and $-\frac{t_{21}}{t_{22}} \in \hat{K}^*$ satisfies the Riccati equation.

2. If u is a solution of the Riccati equation then let $T = \begin{pmatrix} 1-u & 1 \\ -u & 1 \end{pmatrix}$. We have $B = \phi(T) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T^{-1} = \begin{pmatrix} u & * \\ 0 & * \end{pmatrix}$ is an upper triangular matrix. Hence G is reducible because of theorem 4.2.8.

If G is completely reducible then according to theorem 4.2.7 there exists a diagonal matrix $D \in Gl(n, \hat{K})$ and a matrix $T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \in Gl(2, \bar{K})$ such that $D = \phi(T) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T^{-1}$. One can easily verify that $t_{11}, t_{12}, t_{21}, t_{22} \neq 0$ and $-\frac{t_{21}}{t_{22}}, -\frac{t_{11}}{t_{12}} \in \bar{K}^*$ satisfy the Riccati equation. Of course $-\frac{t_{21}}{t_{22}} \neq -\frac{t_{11}}{t_{12}}$ because $\det(T) \neq 0$.

3. If u_1, u_2 are the solutions of the Riccati equation then let $T = \begin{pmatrix} -\frac{u_2}{u_1-u_2} & \frac{1}{u_1-u_2} \\ -\frac{u_1}{u_1-u_2} & \frac{1}{u_1-u_2} \end{pmatrix}$.

We have $B = \phi(T) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T^{-1} = \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix}$ is a diagonal matrix. Hence G is completely reducible because of theorem 4.2.8.

If G is an algebraic subgroup of $\{c.Id \mid c \in \bar{\mathbf{Q}}^*\}$ then there exists a matrix $D = \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix}$ with $u \in \bar{K}$ and a matrix $T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \in Gl(2, \hat{K})$ such that $D = \phi(T) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T^{-1}$. One can easily verify that $-\frac{(ct_{21}+dt_{11})}{(ct_{22}+dt_{12})} \in \hat{K}^*$ is a solution of the Riccati equation for $c, d \in \bar{\mathbf{Q}}$ with $c \neq 0$ or $d \neq 0$. And $-\frac{(c_1 t_{21} + d_1 t_{11})}{(c_1 t_{22} + d_1 t_{12})} = -\frac{(c_2 t_{21} + d_2 t_{11})}{(c_2 t_{22} + d_2 t_{12})}$ if and only if $c_1 = c_2 = 0$ or $\frac{d_1}{c_1} = \frac{d_2}{c_2}$.

4. If u_1, u_2, u_3 are three distinct solutions of the Riccati equation then the system $(A) : \phi \mathbf{y} = A \mathbf{y}$ is equivalent with the systems $(B_1), (B_2)$ and

(B_3) corresponding to the matrices $\begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix}, \begin{pmatrix} u_1 & 0 \\ 0 & u_3 \end{pmatrix}$ and $\begin{pmatrix} u_2 & 0 \\ 0 & u_3 \end{pmatrix}$ respectively. From the fact that (B_1) and (B_2) are equivalent it follows that $u_2 = \frac{\phi(f)}{f}u_3$. Hence system (B_3) is equivalent to the system (C) : $\phi(y) = \begin{pmatrix} u_2 & 0 \\ 0 & u_2 \end{pmatrix}y$ and G is an algebraic subgroup of $\{c.Id \mid c \in \bar{\mathbf{Q}}^*\}$ according to theorem 4.2.8. From the proof of statement 3 it follows that the Riccati equation has infinitely many solutions.

Our task is to make an algorithm which computes all solutions $u \in \hat{K}^*$ of the Riccati equation. The algorithm consists of a few steps.

1. First we compute the first two terms of all possible local formal solutions at ∞ . Let $t = 1/z$. Let ϕ be the automorphism of $\bar{\mathbf{Q}}((t))$ given by $\phi(t) = \frac{t}{t+1}$. Then ϕ coincides with our former ϕ on $\bar{\mathbf{Q}}(t) = \bar{\mathbf{Q}}(z)$. For the moment we consider a and b as Laurent series in t with coefficients in k .

We define the discrete valuation $v : \bar{\mathbf{Q}}((t)) \rightarrow \mathbf{Z}$ in the usual way by $v(\sum_{n=-\infty}^{\infty} c_n t^n) = \min\{n \mid c_n \neq 0\}$. In particular $v(0) = \infty$. Elementary properties of v are $v(u_1 u_2) = v(u_1) + v(u_2)$ and $v(u_1 + u_2) \geq \min(v(u_1), v(u_2))$. Hence if $v(u_1) \neq v(u_2)$ then $v(u_1 + u_2) = \min(v(u_1), v(u_2))$. Another property of v is that $v(u) = v(\phi u)$.

We distinguish two cases.

- (a) $2v(a) < v(b)$. In this case there are exactly two solutions $u, \tilde{u} \in k((t))$ of the Riccati equation. The first solution u satisfies $v(au) = v(u\phi(u)) < v(b)$ and $v(u) = v(a)$ and the other solution $\tilde{u}$ satisfies $v(a\tilde{u}) = v(b) < v(\tilde{u}\phi(\tilde{u}))$ and $v(\tilde{u}) = v(b) - v(a)$. We can compute succesively the coefficients of u and $\tilde{u}$ by simply solving linear equations with coefficients in k . Hence no field extension of k is needed.
- (b) $v(b) \leq 2v(a)$. If $v(b)$ is odd then there is clearly no solution of the Riccati equation. If $v(b)$ is even and $u \in \bar{k}((t))$ satisfies the Riccati equation then we have $v(b) = v(u\phi(u)) \leq v(au)$ and $v(u) = \frac{1}{2}v(b)$. Let $l = \frac{1}{2}v(b)$. We write $a = \sum_{n=l}^{\infty} a_n t^n$ ($a_l = 0$ is allowed), $b = \sum_{n=2l}^{\infty} b_n t^n$ and $u = \sum_{n=l}^{\infty} u_n t^n$ and try to solve the equation $(\dagger) : u\phi(u) + au + b = 0$.

The $(2l)^{th}$ -coefficient of $(\dagger)$ gives us the equation $u_l^2 + a_l u_l + b_{2l} = 0$. Let $D = a_l^2 - 4b_{2l}$. If $D \neq 0$ then we find two solutions $u_l \in k(\sqrt{D})$ of the quadratic equation. If $D = 0$ then we find exactly one solution $u_l \in k$ of the quadratic equation.

The $(2l+1)^{th}$ -coefficient of $(\dagger)$ gives us the equation $(2u_l + a_l)u_{l+1} - lu_l^2 + a_{l+1}u_l + b_{2l+1} = 0$.

If $D \neq 0$ then $2u_l + a_l \neq 0$. And we find for both values of u_l one value $u_{l+1} \in k(\sqrt{D})$.

If $D = 0$ then $2u_l + a_l = 0$. In this case if $-lu_l^2 + a_{l+1}u_l + b_{2l+1} \neq 0$ there is no solution $u \in \bar{\mathbf{Q}}((t))$ of the Riccati equation. If $-lu_l^2 + b_{2l+1} + a_{l+1}u_l = 0$ then we can compute one or two values for u_{l+1} in at worst a quadratic field extension of k by solving the quadratic equation $u_{l+1}^2 - ((2l+1)u_l - a_{l+1})u_{l+1} + (\frac{1}{2}l(l+1)u_l + a_{l+2})u_l + b_{2l+2} = 0$ which is given by the $(2l+2)^{th}$ -coefficient of $(\dagger)$.

Let S_u be the set of all possibilities for the first two terms of u of its Laurent expansion in t . We discovered that $\#S_u \leq 2$, even if the Riccati equation has infinitely many solutions $u \in \bar{k}(t)$. If we needed a quadratic extension in our computations then we will denote this quadratic extension for future use by k_2 , otherwise $k_2 = k$.

2. In this part of the algorithm we will determine the solutions $u \in k_2(z)$ of the Riccati equation. We rewrite the Riccati equation as $Fu\phi(u) + Gu + H = 0$, where $F, G, H \in k[z]$ and $\gcd(F, G, H) = 1$. Write $u = c\frac{P}{Q}$ with $c \in \bar{\mathbf{Q}}$, $\gcd(P, Q) = 1$ and P, Q monic. Let R denote the greatest monic divisor of Q such that $\phi(R)$ divides P . Then one can write $u = c\frac{\phi(R)p}{Rq}$, where p, q are monic polynomials, $\gcd(p, \phi(q)) = 1$ and $\gcd(\phi(R)p, Rq) = 1$. The Riccati equation reads now:

$$(\dagger) : c^2 F \phi^2(R) \phi(p) p + c G \phi(R) \phi(q) p + H R \phi(q) q = 0.$$

Hence p is a monic divisor of H and q is a monic divisor of $\phi^{-1}(F)$. We define the sets $S_p = \{p \in k_2[z] \mid p \text{ monic and } p|H\}$ and $S_q = \{q \in k_2[z] \mid q \text{ monic and } q|\phi^{-1}(F)\}$.

Let e be the degree of the polynomial R . Writing $\frac{\phi(R)}{R}$ as a Laurent series in t we get $\frac{\phi(R)}{R} = 1 + et + O(t^2)$, where $O(t^2)$ stands for the higher order terms. $\frac{\phi(R)}{R}$ must be equal to $\frac{uq}{cp}$. So for every possible combination $u \in S_u$, $p \in S_p$ and $q \in S_q$ with $v(u) + v(q) - v(p) = 0$ we compute an $e \in k_2$ from $\frac{uq}{cp} = 1 + et + O(t^2)$. If $e \in \mathbf{Z}_{\geq 0}$ then we write $R = z^e + r_{e-1}z^{e-1} + \dots + r_1z + r_0$ with indeterminates $r_0, r_1, \dots, r_{e-1}$. After substituting this R in $(\dagger)$ we are left with a set of linear equations in the r_i . In this way we find all possible solutions $u \in k_2(z)$ of the Riccati equation. This ends this part of the algorithm.

3. In step 2 we have determined all solutions $u \in k_2(z)$ of the Riccati equation. Now we have to face the problem whether it is possible that there exist solutions $u \in \bar{\mathbf{Q}}(z)$ if there are no solutions $u \in k_2(z)$. A priori this is possible because $\phi^{-1}F$ and H need not split in linear factors in $k_2[z]$. But it is also clear from the construction in step 2 that if the Riccati equation

has a solution in $\bar{\mathbf{Q}}(x)$, there is also a solution in $l(x)$, where $l \supseteq k_2$ is the smallest field which contains the splitting fields of $\phi^{-1}F$ and H . But we have even a stronger rationality result. (Compare with [HP94], where a similar result is derived for differential equations.)

Theorem 4.4.3 *If the Riccati equation has a solution in $\bar{\mathbf{Q}}(z)$ then there is also a solution in a field $\tilde{k}(z)$ with $[\tilde{k} : k] \leq 2$.*

Proof. Let U be the set of solutions of the Riccati equation in $l(x)$. The group $\text{Gal}(l/k)$ acts on the set U . If $\#U = 1$, say $U = \{u\}$, then u is invariant under $\text{Gal}(l/k)$. Hence $u \in k(z)$. If $\#U = 2$ then the kernel of the map $\text{Gal}(l/k) \rightarrow \text{Aut}(U)$ is a subgroup of index ≤ 2 . Hence $u \in \tilde{k}(z)$, where $\tilde{k}(z)$ is a field extension such that $[\tilde{k} : k] \leq 2$. Suppose that $\#U = \infty$. According to Theorems 4.4.2 part 4 and 4.2.8 there exists a $T \in \text{Gl}(2, \bar{\mathbf{Q}}(z))$ such that $\phi(T) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T^{-1} = \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix}$ for some $u \in \bar{\mathbf{Q}}(z)$. Suppose $\sigma \in \text{Gal}(\bar{\mathbf{Q}}/k)$ then $\phi(\sigma(T)) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} (\sigma(T))^{-1} = \begin{pmatrix} \sigma(u) & 0 \\ 0 & \sigma(u) \end{pmatrix}$. There is a $g_\sigma \in \bar{\mathbf{Q}}(z)^*$ such that $\sigma(u) = \frac{\phi(g_\sigma)}{g_\sigma} u$. This g_σ is uniquely determined if we require that the numerator and denominator of g_σ are monic. The map $\sigma \mapsto g_\sigma$ is a 1-cocycle. Hilbert 90 states that this 1-cocycle is trivial. See for instance [Ser68]. So we can replace u by $\tilde{u} = \frac{\phi(h)}{h} u$ for a certain $h \in \hat{K}^*$ such that $\tilde{u}$ is invariant under $\text{Gal}(\bar{\mathbf{Q}}/k)$. Hence $\tilde{u} \in k(z)$. Let $\tilde{T} = hT$. Then $\phi(\tilde{T}) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \tilde{T}^{-1} = \begin{pmatrix} \tilde{u} & 0 \\ 0 & \tilde{u} \end{pmatrix}$. Suppose that $C^{-1}\tilde{T}$ in $\text{Gl}(2, \bar{\mathbf{Q}}(z))$ also satisfies $\phi(C^{-1}\tilde{T}) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} (C^{-1}\tilde{T})^{-1} = \begin{pmatrix} \tilde{u} & 0 \\ 0 & \tilde{u} \end{pmatrix}$. Then $\phi(C) = C$ and so $C \in \text{Gl}(2, \bar{\mathbf{Q}})$. For $\sigma \in \text{Gal}(\bar{\mathbf{Q}}/k)$ one has therefore $\sigma(\tilde{T}) = C_\sigma^{-1}\tilde{T}$ for some $C_\sigma^{-1} \in \text{Gl}(2, \bar{\mathbf{Q}})$. The map $\sigma \mapsto C_\sigma$ is a 1-cocycle for $\text{Gal}(\bar{\mathbf{Q}}/k)$ acting on $\text{Gl}(2, \bar{\mathbf{Q}})$. According to [Ser68] this 1-cocycle is trivial. This means that $S = C^{-1}\tilde{T}$ is invariant under $\text{Gal}(\bar{\mathbf{Q}}/k)$ for a certain $C \in \text{Gl}(2, \bar{\mathbf{Q}})$. It follows that $S \in \text{Gl}(2, k(z))$. In particular the Riccati equation has (infinitely many) solutions in $k(z)$. $\square$

So if $k_2 = k$, then we want to determine all fields $\tilde{k} \subset l$ with $[\tilde{k} : k] \leq 2$. It is obvious that $\tilde{k}$ must be of the form $k(\sqrt{s})$, where s is an algebraic integer in l . Recall that l is the splitting field of the polynomial FH . After a suitable linear substitution $z \mapsto \frac{z}{n}$, where $n \in \mathbf{Z}_{\geq 1}$ we can assume that FH is monic and that the coefficients of FH are algebraic integers. s must be a divisor of the discriminant of this polynomial. This gives us a finite set of possible quadratic extensions $k(\sqrt{s})$ of k in l . For each possible quadratic extension $\tilde{k}$ we determine the sets $S_p = \{p \in \tilde{k}[z] \mid p \text{ monic and } p|H\}$ and $S_q = \{q \in \tilde{k}[z] \mid q \text{ monic and } q|\phi^{-1}(F)\}$. After that we proceed as in 2.

As we will see in Subsection 4.5.2 step 3 of the algorithm is not superfluous. That means, if we did not need a quadratic extension of our field of constants in step 1, it is possible that we really need a quadratic extension of our field of constants in step 3 for solving the Riccati equation. We will provide an explicit example in Subsection 4.5.2.

4.4.2 G is reducible

If the Riccati equation has a solution in $\hat{K}$, then we can compute an equivalent system $(A) : \phi \mathbf{y} = A\mathbf{y}$, where A has the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Moreover we can assume that $b = 0$ if the Riccati equation has two or infinitely many solutions. We denote by U the subgroup of $Gl(2, \bar{\mathbf{Q}})$ consisting of upper triangular matrices and by D the subgroup of diagonal matrices.

Lemma 4.4.4 *The reducible subgroups $G \subset Gl(2, \bar{\mathbf{Q}})$ with G/G^0 finite cyclic are*

1. *The zero-dimensional groups*

$$D_{k,l,e} = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in D \mid \alpha^k = 1, \delta^l = 1, \alpha^{eg_\alpha} \delta^{g_\delta} = 1 \right\}$$

and the one-dimensional groups

$$U_{k,l,e} = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in U \mid \alpha^k = 1, \delta^l = 1, \alpha^{eg_\alpha} \delta^{g_\delta} = 1 \right\}$$

for $l, k, e \in \mathbf{Z}_{\geq 1}$ with $\gcd(k, l, e) = 1$, where $g_\alpha = \frac{k}{\gcd(k, l)}$ and $g_\delta = \frac{l}{\gcd(k, l)}$.

2. *The one-dimensional groups*

$$D_{m,n} = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in D \mid \alpha^m \delta^n = 1 \right\}$$

and the two-dimensional groups

$$U_{m,n} = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in U \mid \alpha^m \delta^n = 1 \right\}$$

for $n, m \in \mathbf{Z}$

3. *The two-dimensional group D and the three-dimensional group U .*

Proof. If $G \subset D$ is a zero-dimensional subgroup with G/G^0 finite cyclic then G is a subgroup of $\tilde{D}_{k,l} = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in D \mid \alpha^k = 1, \delta^l = 1 \right\}$ with $k, l \in \mathbf{Z}_{\geq 1}$. Note that $\tilde{D}_{k,l}$ is isomorphic to $\mathbf{Z}/l\mathbf{Z} \times \mathbf{Z}/k\mathbf{Z}$ as an abstract group. Assume that k, l are

minimal with respect to the condition that $G \subseteq \tilde{D}_{k,l}$. Then $G \cong \mathbf{Z}/lcm(k,l)\mathbf{Z}$ because G is cyclic and G contains elements of order l and of order k but G does not contain elements of order greater than $lcm(l,k)$. The subgroups of $\tilde{D}_{k,l}$ which are isomorphic to $\mathbf{Z}/lcm(k,l)\mathbf{Z}$ as abstract groups are the groups $D_{k,l,e} = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in D \mid \alpha^k = 1, \delta^l = 1, \alpha^{eg_\alpha} \delta^{g_\delta} = 1 \}$ with $l, k, e \in \mathbf{Z}_{\geq 1}$ and $gcd(k, l, e) = 1$, where $g_\alpha = \frac{k}{gcd(k,l)}$ and $g_\delta = \frac{l}{gcd(k,l)}$.

If G a one-dimensional algebraic subgroup of D then G is equal to a group $D_{m,n} = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in D \mid \alpha^m \delta^n = 1 \}$ with $m, n \in \mathbf{Z}$. For all $m, n \in \mathbf{Z}$ we have $D_{m,n}/D_{m,n}^0$ is finite cyclic.

If G is a two-dimensional subgroup of D then $G = D$.

The classification of the reducible but not completely reducible subgroups $G \subseteq U$ with G/G^0 finite cyclic is analogous to the classification of the completely reducible subgroups $G \subseteq D$ with G/G^0 finite cyclic. $\square$

The algorithm continues as follows. Suppose the Riccati equation has exactly one solution in $\hat{K}$. Then the difference Galois group G is reducible but not completely reducible. If G is a proper subgroup of U , then according to Theorem 4.2.7 there must be a matrix $T = \begin{pmatrix} f & g \\ 0 & h \end{pmatrix} \in U(\hat{K})$ such that $B = \phi(T)AT^{-1} = \begin{pmatrix} a \frac{\phi(f)}{f} & * \\ 0 & d \frac{\phi(h)}{h} \end{pmatrix} \in G(\hat{K})$.

First we want to determine whether the difference Galois group is one of the one-dimensional groups described in part 1 of Lemma 4.4.4. We apply the algorithm for first difference equations to a and d . This yields a new equivalent system $\tilde{A} = \begin{pmatrix} \tilde{a} & * \\ 0 & \tilde{d} \end{pmatrix}$, where $\tilde{a}$ and $\tilde{d}$ are reduced.

If $\tilde{a}$ and $\tilde{d}$ are constant then the system $\tilde{A}$ is already in standard form. If both $\tilde{a}$ and $\tilde{d}$ are roots of unity, then the difference Galois group is one of the groups $U_{k,l,e}$. Otherwise G is one of the groups described in part 2 or part 3 of lemma 4.4.4.

Suppose now that that $\tilde{a}$ or $\tilde{d}$ is not constant. Then the difference Galois group is not a group described in part 1 of Lemma 4.4.4.

If $\tilde{a}$ is constant and $\tilde{d}$ is not constant then the system $(\tilde{A})$ is already in standard form. The difference Galois group G is the group $U_{n,0}$, if $\tilde{a}$ is an n th primitive root of unity. Otherwise the difference Galois group G is the group U .

If $\tilde{d}$ is constant and $\tilde{a}$ is not constant then the system $(\tilde{A})$ is also already in standard form. The difference Galois group G is the group $U_{0,n}$, if $\tilde{d}$ is an n th primitive root of unity. Otherwise the difference Galois group G is the group U .

Suppose now that both $\tilde{a}$ and $\tilde{d}$ are reduced but not constant. The difference Galois group is one of the groups $U_{m,n}$ if and only if there exists $r, s \in \mathbf{Z} \setminus \{0\}$

with $\gcd(r, s) = 1$ and an $f \in \bar{K}$ such that $\tilde{a}^r \tilde{d}^s \frac{\phi(f)}{f}$ is a root of unity. Without loss of generality we can assume that $r > 0$. Let N_a and N_d denote the degree of the numerator of $\tilde{a}$ and $\tilde{d}$ respectively and let D_a and D_d denote the degree of the denominator of $\tilde{a}$ and $\tilde{d}$ respectively.

Suppose first that there exist $r, s \in \mathbf{Z}_{\geq 1}$ with $\gcd(r, s) = 1$ and an $f \in \hat{K}$ such that $\tilde{a}^r \tilde{d}^s \frac{\phi(f)}{f}$ is constant. Then we must have $rD_a = sN_d$ and $rN_a = sD_d$, because $\tilde{a}$ and $\tilde{d}$ are reduced.

If $rD_a = sN_d$ and $rN_a = sD_d$ holds then we apply the algorithm for first order difference equations to $\tilde{a}^r \tilde{d}^s$ to investigate whether there exist an $f \in \hat{K}$ such that $\tilde{a}^r \tilde{d}^s \frac{\phi(f)}{f}$ is constant. If there exist such an f then we let $T = \begin{pmatrix} f^v & 0 \\ 0 & f^w \end{pmatrix}$, where

v, w are chosen such that $vr + ws = 1$. Then $B = \phi(T)\tilde{A}T^{-1}$ is in standard form.

Suppose now that there exists an $r \in \mathbf{Z}_{\geq 1}$ and an $s \in \mathbf{Z}_{\leq -1}$ with $\gcd(r, s) = 1$ and an $f \in \hat{K}$ such that $\tilde{a}^r \tilde{d}^s \frac{\phi(f)}{f}$ is constant. Then we must have $rN_a = -sN_d$ and $rD_a = -sD_d$, because $\tilde{a}$ and $\tilde{d}$ are reduced.

If $rN_a = -sN_d$ and $rD_a = -sD_d$ holds then we apply the algorithm for first order difference equations to $\tilde{a}^r \tilde{d}^s$ to investigate whether there exist an $f \in \hat{K}$ such that $\tilde{a}^r \tilde{d}^s \frac{\phi(f)}{f}$ is constant. If there exist such an f then we let $T = \begin{pmatrix} f^v & 0 \\ 0 & f^w \end{pmatrix}$,

where v, w are chosen such that $vr + ws = 1$. Then $B = \phi(T)\tilde{A}T^{-1}$ is in standard form.

If none of the two cases above holds then the system $(\tilde{A})$ is already in standard form and the difference Galois group is the upper triangular group U .

We will not discuss the completely reducible case because this case is analogous to the reducible but not completely reducible case.

4.4.3 G is imprimitive

If we did not find a solution $u \in \hat{K}^*$ for the Riccati equation then the difference Galois group is irreducible. A group G is called imprimitive if $G \subseteq F = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid \alpha\delta \neq 0 \} \cup \{ \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \mid \beta\gamma \neq 0 \}$. In this subsection we determine whether G is imprimitive if we know already that G is not reducible.

Lemma 4.4.5 *Suppose that the difference Galois group G of the difference equation $(\#) : \phi^2 y + a\phi y + by = 0$ is irreducible. Then the following statements are equivalent.*

1. G is an imprimitive group.
2. There exists an $r \in \hat{K}^*$ such that the equations $(\#)$ and $\phi^2 y + ry = 0$ are equivalent.

Proof. $1 \Rightarrow 2$. If G is imprimitive and not reducible then according to Theorems 4.2.7 and 4.2.8 there is a system $(B) : \phi \mathbf{y} = B\mathbf{y}$ where B is of the form $\begin{pmatrix} 0 & f \\ g & 0 \end{pmatrix}$ such that (B) and $(\#)$ are equivalent. Let $T = \begin{pmatrix} 1 & 0 \\ 0 & f \end{pmatrix}$. Then $\phi(T)BT^{-1} = \begin{pmatrix} 0 & 1 \\ \phi(f)g & 0 \end{pmatrix}$. This matrix corresponds to a second order equation of the right form.

$2 \Rightarrow 1$. The difference equation $\phi^2 y + ry = 0$ is obviously imprimitive because of theorem 4.2.8. $\square$

Suppose now that the equations $(\#) : \phi^2 y + a\phi y + by = 0$ with $a \neq 0$ and $\phi^2 y + ry = 0$ are equivalent. Then there exist $c, d \in \hat{K}^*$ such that y is a solution of $(\#)$ if and only if $cy + d\phi y$ is a solution of $\phi^2 y + ry = 0$. In this case $\frac{c}{d}y + \phi y$ satisfies the equation $\phi^2 y + \frac{d}{\phi^2(d)}ry = 0$.

Theorem 4.4.6 *Suppose that the difference Galois group G of the equation $(\#) : \phi^2 y + a\phi y + by = 0$, $a \neq 0$ is irreducible. Then G is imprimitive if and only if there exists a solution $E \in \hat{K}^*$ of the Riccati equation*

$$(\#\#) : \quad \phi^2(E)E + \left(\phi^2\left(\frac{b}{a}\right) - \phi(a) + \frac{\phi(b)}{a}\right)E + \frac{\phi(b)b}{a^2} = 0.$$

And if $E \in \hat{K}^*$ is a solution of this Riccati equation then y satisfies the equation $(\#)$ if and only if $Dy + \phi y$ satisfies the equation $\phi^2 y + ry = 0$, where $D = E + \frac{b}{a}$ and $r = -a\phi(a) + \phi(b) + a\phi^2(D)$.

Proof. If G is imprimitive and y satisfies the equation $(\#)$ then there exists an $D \in \hat{K}^*$ such that $Dy + \phi y$ satisfies an equation of the form $\phi^2 y + ry = 0$, where $r \in \hat{K}^*$. We have $\phi^2(Dy + \phi(y)) = (\phi(a)b - b\phi^2(D))y + (a\phi(a) - \phi(b) - a\phi^2(D))\phi(y)$. The group G is irreducible. Hence y and $\phi(y)$ are linearly independent over $\hat{K}$. Therefore we must have $\phi(a)b - b\phi^2(D) = -rD$ and $a\phi(a) - \phi(b) - a\phi^2(D) = -r$. After eliminating r we get the equation $\phi^2(D)D - \frac{b}{a}\phi^2(D) - \phi(a)D + \frac{\phi(b)}{a}D + \frac{\phi(a)b}{a} = 0$ for D . Let $E = D - \frac{b}{a}$. Then E satisfies the Riccati equation $\phi^2(E)E + \left(\phi^2\left(\frac{b}{a}\right) - \phi(a) + \frac{\phi(b)}{a}\right)E + \frac{\phi(b)b}{a^2} = 0$.

Conversely if E satisfies the Riccati equation $\phi^2(E)E + \left(\phi^2\left(\frac{b}{a}\right) - \phi(a) + \frac{\phi(b)}{a}\right)E + \frac{\phi(b)b}{a^2} = 0$ then $Dy + \phi y$ satisfies the equation $\phi^2 y + ry = 0$ if y satisfies the equation $(\#)$ where $D = E + \frac{b}{a}$ and $r = -a\phi(a) + \phi(b) + a\phi^2(D)$. $\square$

Remark 4.4.7 *We can find the rational solutions of equation $(\#\#)$ as follows. Let $\tau : \hat{K} \rightarrow \hat{K}$ be the $\bar{\mathbf{Q}}$ -linear map given by $z \mapsto 2z$. Then $\tau \circ \phi^2 = \phi \circ \tau$. If we apply τ to the equation $(\#\#)$ then we get the equation*

$$\phi(\tau(E))\tau(E) + \tau\left(\phi^2\left(\frac{b}{a}\right) - \phi(a) + \frac{\phi(b)}{a}\right)\tau(E) + \tau\left(\frac{\phi(b)b}{a^2}\right) = 0.$$

We can find all the rational solutions $\tau(E)$ of this equation by applying the algorithm described in Subsection 4.4.1. Then we apply τ^{-1} to these solutions and we find the actual rational solutions of the equation (##) appearing in Theorem 4.4.6.

Lemma 4.4.8 *The imprimitive subgroups $G \subset Gl(2, \bar{\mathbf{Q}})$ with G/G^0 finite cyclic are*

1. $F = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid \alpha\delta \neq 0 \} \cup \{ \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \mid \beta\gamma \neq 0 \}$.
2. $H_n^- = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid (\alpha\delta)^n = 1 \} \cup \{ \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \mid (\beta\gamma)^n = -1 \}$ for $n \in \mathbf{Z}_{\geq 1}$.
3. $H_n^+ = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid (\alpha\delta)^n = 1 \} \cup \{ \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \mid (\beta\gamma)^n = 1 \}$ for n odd.

Proof. If G is an imprimitive group with G/G^0 finite cyclic then $G \cap D = D$ or $G \cap D = D_{m,n}$ for $m, n \in \mathbf{Z} \setminus \{0\}$ (See Subsection 4.4.2). If $\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in G$ and $\begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \in G$ then also $\begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix}^{-1} = \begin{pmatrix} \delta & 0 \\ 0 & \alpha \end{pmatrix}$. So if $G \cap D = D_{m,n}$ for $m, n \in \mathbf{Z} \setminus \{0\}$ then $m = n$ or $m = -n$. A calculation shows that the second possibility does not yield any imprimitive subgroup with G/G^0 finite cyclic and the first possibility yields the groups H_n^- for $n \in \mathbf{Z}_{\geq 1}$ and H_n^+ for n odd. $\square$

Consider the system $\phi(\mathbf{y}) = \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} \mathbf{y}$. We can apply the algorithm for first order difference equations to cd . Then we will find a $f \in \hat{K}^*$ such that $cd \frac{\phi(f)}{f}$ is reduced. Let $T = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}$. Then $B = \phi(T) \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} T^{-1}$ is in standard form.

4.4.4 G contains $Sl(2, \bar{\mathbf{Q}})$

Consider the system $\phi(\mathbf{y}) = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \mathbf{y}$. If the difference Galois group G of this system is neither reducible nor imprimitive, then $G = Gl(2, \bar{\mathbf{Q}})$ or $G = Sl(2, \bar{\mathbf{Q}})_n = \{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid (\alpha\delta - \beta\gamma)^n = 1 \}$. We apply the algorithm for first order difference equations to $b = \det \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix}$ and find an $f \in \hat{K}^*$ such that $\frac{\phi(f)}{f} b$ is reduced. Let $T = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}$. Then $B = \phi(T) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T^{-1}$ is in standard form. This finishes the algorithm.

4.5 Examples

In subsection 4.5.1 sequences spaces are used in order to make the Picard–Vessiot rings associated to a system of difference equations more concrete. The explicit solutions which can be computed are certain sequences which will be called Liouvillian. Some concrete examples will be given.

In subsection 4.5.2 we will demonstrate how one can construct examples where a quadratic field extension of the field of constants is needed for solving the Riccati equation.

4.5.1 Sequences spaces

Let F be any field. Consider the set of sequences $F^{\mathbf{N}}$. This set forms a ring by using coordinate-wise addition and multiplication. Let J be the ideal of sequences with at most finitely many non-zero terms. Then we define $\mathcal{S}_F = F^{\mathbf{N}}/J$. The map $\rho : \mathcal{S}_F \rightarrow \mathcal{S}_F$ given by $\rho((a_1, a_2, a_3, \dots)) = (a_2, a_3, \dots)$ is well defined on equivalence classes. Moreover, ρ is an automorphism of the ring $\mathcal{S}_F$. For simplicity we will identify an element $\mathbf{a} = (a_1, a_2, a_3, \dots)$ with its equivalence class.

Let C be any field of characteristic zero. (We are interested in the case that $C = \bar{\mathbf{Q}}$ or $C = k$, where k is an algebraic number field). The rational function field $C(z)$ can be embedded in $\mathcal{S}_C$ by mapping a rational function f to the sequence $\mathbf{s}_f = (s_1, s_2, \dots)$ where $s_n = f(n)$ for all but finitely many $n \in \mathbf{N}$. We will denote this map $f \mapsto \mathbf{s}_f$ by ψ and, following [Pet92], we will denote the image of ψ in $\mathcal{S}_C$ by $\mathcal{R}_C$.

Lemma 4.5.1 *The map $\psi : C(z) \rightarrow \mathcal{R}_C$ is an isomorphism of difference fields.*

Proof. Two rational functions that agree on infinitely many arguments are identical. Further more, it is obvious that $\psi\phi = \rho\psi$. $\square$

From now on we will identify rational functions $f \in C(z)$ and their images $\mathbf{s}_f$ in $\mathcal{R}_C$.

Theorem 4.5.2 *Consider the system of difference equations $(A) : \phi(\mathbf{y}) = A\mathbf{y}$, where $A \in Gl(n, \bar{\mathbf{Q}}(z))$. There is a difference subring $R \subset \mathcal{S}_{\bar{\mathbf{Q}}}$ such that R is a Picard–Vessiot extension associated to the system (A) . Moreover, if $A \in Gl(n, k(z))$, where k is an algebraic number field, then there exists already a basis of the solution space consisting of elements in $(\mathcal{S}_k)^n$.*

Proof. We refer to chapter 4 of [PS96]. $\square$.

Remark 4.5.3 *Above theorem shows that there is a natural rational k -structure on the vectorspace of solutions. Hence it is possible to develop Galois theory of difference equations over a rational function field with a constant field which is not*

algebraically closed. Compare with [HP95], where a similar theory is developed for the differential case.

From now on we will write for simplicity $\mathcal{S}$ instead of $\mathcal{S}_{\bar{\mathbf{Q}}}$ and ϕ instead of ρ .

Definition 4.5.4 We define the ring of Liouvillian sequences $\mathcal{L}$ recursively. $\mathcal{L}$ is the smallest subring of $\mathcal{S}$ such that

1. $\hat{K} \subset \mathcal{L}$.
2. $\mathbf{a} \in \mathcal{L}$ implies that $\phi(\mathbf{a}) \in \mathcal{L}$
3. $\mathbf{a} \in \hat{K}$ implies that $\mathbf{b} \in \mathcal{L}$ if $b_{n+1} = a_n b_n$ for all but finitely many $n \in \mathbf{N}_{\geq 1}$.
4. $\mathbf{a} \in \mathcal{L}$ implies that $\mathbf{b} \in \mathcal{L}$ if $b_{n+1} = a_n + b_n$ for all but finitely many $n \in \mathbf{N}_{\geq 1}$.
5. $\mathbf{a} \in \mathcal{L}$ implies that $\mathbf{b} \in \mathcal{L}$ if there exist a $j \in \mathbf{N}_{\geq 1}$ such that $b_{jn} = a_n$ and $b_n = 0$ if $n \not\equiv 0 \pmod{j}$. In this case we call $\mathbf{b}$ an j -interlacing of $\mathbf{a}$ with zeroes.

Theorem 4.5.5 Suppose $\mathbf{a} \in \mathcal{S}$. Then the following statements are equivalent.

1. $\mathbf{a} \in \mathcal{L}$
2. The sequence $\mathbf{a}$ satisfies a linear difference equation over $\hat{K}$ so that the difference Galois group G associated to this equation is solvable.

Proof. $2 \Rightarrow 1$. Consider the system of difference equations $(A) : \phi(\mathbf{y}) = A\mathbf{y}$, where $A \in Gl(n, \hat{K})$. Let $V_A = \{\mathbf{y} \in \mathcal{S}^n \mid \phi(\mathbf{y}) = A\mathbf{y}\}$ be the solution space for the system of difference equations (A) . We will prove that if the difference Galois group associated to this system is solvable then V_A is an n -dimensional $\bar{\mathbf{Q}}$ -linear subspace of $\mathcal{L}^n$. This statement is slightly more general than the $2 \Rightarrow 1$ part of the theorem.

Suppose now that the difference Galois group is solvable and G/G^0 is finite cyclic of order m . We assume that system (A) is already in standard form, that is $A \in G(\hat{K})$. This is without loss of generality because if $(\tilde{A}) : \phi(\mathbf{y}) = \tilde{A}\mathbf{y}$ is an equivalent system of difference equations then we have $V_A \subset \mathcal{L}^n$ if and only if $V_{\tilde{A}} \subset \mathcal{L}^n$.

Let $B = \phi^{m-1}(A) \cdots \phi(A)A$. Obviously $B \in G^0(\hat{K})$. Because of the Lie-Kolchin theorem we can assume that B is an upper triangular matrix. Namely if B is not yet an upper triangular then according to the Lie-Kolchin theorem there exists a matrix $T \in Gl(n, \bar{\mathbf{Q}})$ so that $\tilde{B} = T^{-1}BT$ is an upper triangular matrix and then we continue with $\tilde{B}$ instead of B . Consider the system of difference equations $(B) : \phi^m(\mathbf{y}) = B\mathbf{y}$. The solution space $V_B = \{\mathbf{y} \in \mathcal{S}^n \mid \phi^m(\mathbf{y}) = B\mathbf{y}\}$ of this system of difference equations is an nm -dimensional $\bar{\mathbf{Q}}$ -linear space and it is obvious that $V_A \subset V_B$. We will prove that $V_B \subset \mathcal{L}^n$. Let $\mathcal{S}_i = \{\mathbf{a} \in \mathcal{S} \mid a_j =$

0 if $j \not\equiv i \pmod{m}$ for $i = 0, \dots, m-1$. Then we have $\mathcal{S} = \mathcal{S}_0 \oplus \dots \oplus \mathcal{S}_{m-1}$. Let $V_B^i = V_B \cap \mathcal{S}_i^n$ for $i = 0, \dots, m-1$. Then V_B^i is an n -dimensional $\bar{\mathbf{Q}}$ -linear space for $i = 0, \dots, m-1$ and $V_B = V_B^0 \oplus \dots \oplus V_B^{m-1}$.

Let $\tau : \hat{K} \rightarrow \hat{K}$ be the $\bar{\mathbf{Q}}$ -linear map given by $z \mapsto mz$. Then $\tau \circ \phi^m = \phi \circ \tau$. Let $C = \tau B \in Gl(n, \hat{K})$. Note that C is also an upper triangular matrix. Consider the system of linear difference equations $(C) : \phi(\mathbf{y}) = C\mathbf{y}$. The solution space V_C is n -dimensional. We have $\mathbf{v} \in V_C$ if and only if $\mathbf{w} \in V_B^0$, where $\mathbf{w}$ is an m -interlacing of $\mathbf{v}$ with zeroes. We will show by incomplete induction that there exists an upper triangular fundamental matrix $U = (u_{ij}) \in Gl(n, \mathcal{L})$ for the system of difference equations (C) . Let $u_{ii} \in \mathcal{S}$ be a nonzero solution of the first order difference equation $\phi(y) = c_{ii}y$ for $i = 1, \dots, n$. Obviously $u_{ii} \in \mathcal{L}$ for $i = 1, \dots, n$. Moreover it is obvious that u_{ii} is an invertible element of $\mathcal{L}$ for $i = 1, \dots, n$. If $t \in \mathcal{S}$ satisfies $\phi(t) - t = \frac{c_{12}u_{22}}{c_{11}u_{11}}$ then also $t \in \mathcal{L}$. Let $u_{12} = tu_{11}$. Then u_{12} satisfies $\phi(u_{12}) = c_{11}u_{12} + c_{12}u_{22}$ and $u_{12} \in \mathcal{L}$. In more or less the same way one can construct $u_{ij} \in \mathcal{L}$ for all $i < j$ so that $U = (u_{ij})$ is a fundamental matrix for system (C) . We conclude that $V_C \subset \mathcal{L}^n$ and therefore $V_B^0 \subset \mathcal{L}^n$. By similar constructions one can show that $V_B^i \subset \mathcal{L}^n$ for $i = 1, \dots, m-1$. Hence $V_B \subset \mathcal{L}^n$ and $V_A \subset \mathcal{L}^n$.

1 $\Rightarrow$ 2. We will prove this part of the theorem case by case.

1. Suppose $\mathbf{a} \in \hat{K} \setminus \{0\}$. Then $\mathbf{a}$ satisfies the first order linear difference equation $\phi(y) = cy$, where $c = \frac{\phi(\mathbf{a})}{\mathbf{a}}$. The difference Galois group associated to this difference equation is the trivial group.
2. Suppose $\mathbf{a} \in \mathcal{S} \setminus \{0\}$ satisfies a linear difference equation then $\phi(\mathbf{a})$ satisfies an equivalent equation of the same order. Hence the difference Galois groups associated to both equations coincide.
3. Suppose $\mathbf{b} \in \mathcal{S} \setminus \{0\}$ satisfies the first order difference equation $\phi(y) = \mathbf{a}y$, where $\mathbf{a} \in \hat{K} \setminus \{0\}$. Then the difference Galois group G associated to this difference equation is an algebraic subgroup of the multiplicative group $\mathbf{G}_m = \bar{\mathbf{Q}}^*$. Hence the difference Galois group G is solvable.
4. Suppose that L is an n th order linear difference operator with coefficients in $\hat{K}$ so that $L\mathbf{a} = 0$. Let G be the difference Galois group associated to the difference equation $Ly = 0$. Let $\mathbf{b} \in \mathcal{S}$ satisfy $\phi(\mathbf{b}) - \mathbf{b} = \mathbf{a}$. Then $L(\phi - 1)\mathbf{b} = 0$. Hence $\mathbf{b}$ satisfies an $n+1$ th order difference equation and the difference Galois group $\tilde{G}$ associated to this equation is a subgroup of the semidirect product of G and $\bar{\mathbf{Q}}^n$. (Note that G acts on $\bar{\mathbf{Q}}^n$). Hence the group $\tilde{G}$ is solvable if the group G is solvable.
5. Suppose that $\mathbf{a} \in \mathcal{S}$ satisfies the n th order linear difference equation $\phi^n(y) + c_{n-1}\phi^{n-1}(y) + \dots + c_0y = 0$, where $c_0, c_1, \dots, c_{n-1} \in \hat{K}$ and $c_0 \neq 0$.

As usual we will identify this difference equation with the system of differ-

ence equations $\phi(\mathbf{y}) = C\mathbf{y}$, where $C = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{n-1} \end{pmatrix}$.

Let $G \subset Gl(n, \bar{\mathbf{Q}})$ be the difference Galois group associated to this difference equation, then according to theorem 4.2.7 there exists a matrix $T \in Gl(n, \hat{K})$ so that $B = \phi(T)CT^{-1} \in G(\hat{K})$. Now let $\mathbf{b}$ be an m -interlacing of $\mathbf{a}$ with zeroes. Then $\mathbf{b}$ satisfies the nm th order linear difference equation $\phi^{nm}(y) + (\tau^{-1}c_{n-1})\phi^{(n-1)m}(y) + \cdots + (\tau^{-1}c_0)y = 0$, where $\tau : \hat{K} \rightarrow \hat{K}$ is the $\bar{\mathbf{Q}}$ -linear map given by $z \mapsto mz$. Note that $\tau^{-1} \circ \phi = \phi^m \circ \tau^{-1}$. The nm th order linear difference equation for $\mathbf{b}$ can be identified with the $nm \times nm$ sys-

tem of difference equations $\phi(\mathbf{y}) = \tilde{C}\mathbf{y}$, where $\tilde{C} = \begin{pmatrix} 0 & I & 0 & \cdots & 0 \\ 0 & 0 & I & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & & I \\ C & 0 & 0 & \cdots & 0 \end{pmatrix} \in$

$Gl(nm, \hat{K})$. Let $\tilde{T} = \text{diag}(\tau^{-1}T, \phi(\tau^{-1}T), \dots, \phi^{m-1}(\tau^{-1}T)) \in Gl(nm, \hat{K})$.

Then $\tilde{B} = \phi(\tilde{T})\tilde{C}\tilde{T}^{-1} = \begin{pmatrix} 0 & I & 0 & \cdots & 0 \\ 0 & 0 & I & \cdots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & & I \\ \tau^{-1}B & 0 & 0 & \cdots & 0 \end{pmatrix}$. Hence according to the-

orem 4.2.8 the difference Galois group $\tilde{G}$ associated to the linear difference equation for $\mathbf{b}$ is a subgroup of a cyclic extension of order m of m copies of G . Hence if G is a solvable group then $\tilde{G}$ is a solvable group.

We still have to show that if $\mathbf{a}$ and $\mathbf{b}$ satisfy linear difference equations over $\hat{K}$ so that the difference Galois groups associated to these equations are solvable then also $\mathbf{a} - \mathbf{b}$ and $\mathbf{a}\mathbf{b}$ satisfy linear difference equations over $\hat{K}$ so that the difference Galois groups associated to these equations are solvable.

Suppose that the sequence $\mathbf{a}$ satisfies an n th order linear difference equation over $\hat{K}$ and the sequence $\mathbf{b}$ satisfies an m th order linear difference equation. Let $R_{\mathbf{a}}$ and $R_{\mathbf{b}}$ be the Picard–Vessiot extensions associated to the difference equations for $\mathbf{a}$ and $\mathbf{b}$ respectively. Let $V_{\mathbf{a}}$ and $V_{\mathbf{b}}$ be the solution spaces for these equations and let $G_{\mathbf{a}} = DGal(R_{\mathbf{a}}/\hat{K})$ and $G_{\mathbf{b}} = DGal(R_{\mathbf{b}}/\hat{K})$. The difference Galois groups $G_{\mathbf{a}}$ and $G_{\mathbf{b}}$ act faithfully on the solution spaces $V_{\mathbf{a}}$ and $V_{\mathbf{b}}$ respectively. Let $W = \{v_1 + v_2 \mid v_1 \in V_{\mathbf{a}}, v_2 \in V_{\mathbf{b}}\}$. Then W is a $\bar{\mathbf{Q}}$ -linear space of dimension less than or equal than $n + m$. One can construct a linear difference equation whose solution space is W . Let R be the Picard Vessiot extension associated to this equation and let $G = DGal(R/\hat{K})$ be the difference Galois group associated

to this equation. Then G acts on $V_{\mathbf{a}}$ and $V_{\mathbf{b}}$ and G acts faithfully on W . The space W can be considered as a quotient space of $V_{\mathbf{a}} \oplus V_{\mathbf{b}}$. Hence G acts faithfully on $V_{\mathbf{a}} \oplus V_{\mathbf{b}}$. From this it is clear that G is a subgroup of $G_{\mathbf{a}} \times G_{\mathbf{b}}$. Hence the group G is solvable if the groups $G_{\mathbf{a}}$ and $G_{\mathbf{b}}$ are solvable.

Let $\tilde{W} = \text{span}_{\bar{\mathbf{Q}}} \{v_1 v_2 \mid v_1 \in V_{\mathbf{a}}, v_2 \in V_{\mathbf{b}}\}$. Then $\tilde{W}$ is a $\bar{\mathbf{Q}}$ -linear space of dimension less than or equal than nm . One can construct a linear difference equation whose solution space is $\tilde{W}$. Let $\tilde{R}$ be the Picard-Vessiot extension associated to this equation. Obviously $\tilde{R} \subset R$. Hence the difference Galois group $\tilde{G} = D\text{Gal}(\tilde{R}/\tilde{K})$ is solvable if the group G is solvable. $\square$

All the solutions of a second order difference equation $\phi^2 y + a\phi y + by = 0$ are Liouvillian if the difference Galois group is reducible or irreducible and imprimitive. The solutions of a second order difference equation with an imprimitive difference Galois group are not considered to be “closed form” solutions in [Pet92]. Hence our notion of Liouvillian solutions does really extend the notion of “closed form” solutions given in [Pet92]. If the difference Galois group G contains $Sl(2, \bar{\mathbf{Q}})$, then there are no Liouvillian solutions of the second order difference equation $\phi^2 y + a\phi y + by = 0$. Now we give some concrete examples.

Example 1 Consider the equation $\phi^2 y + z\phi y + zy = 0$. First we want to determine the set S_u . Let $t = \frac{1}{z}$. The Riccati equation at ∞ reads $u\phi(u) + \frac{1}{t}u + \frac{1}{t} = 0$. We have $v(\frac{1}{t}) = -1$. So we are in the case $2v(a) < v(b)$. A simple calculation shows that $S_u = \{-\frac{1}{t} + 1 + O(t), -1 - t + O(t^2)\}$. Further we have $S_p = \{1, z\}$ and $S_q = \{1\}$. There are two combinations $u \in S_u$, $p \in S_p$ and $q \in S_q$ such that $v(u) + v(q) - v(p) = 0$. Namely $u = -\frac{1}{t} + 1 + O(t)$, $p = z$, $q = 1$ and $u = -1 - t + O(t^2)$, $p = 1$, $q = 1$. The first combination gives us $-\frac{uq}{p} = 1 - t + O(t^2)$. So $e = -1$. Therefore this combination does not yield a solution $u \in \bar{\mathbf{Q}}(z)$ of the Riccati equation. The second combination gives us $-\frac{uq}{p} = 1 + t + O(t^2)$. Hence $e = 1$. After substituting $c = -1$, $p = 1$, $q = 1$, $R = z + r$ in $(\ddagger)$ we get the equation $z + r + 2 - z(z + r + 1) + z(z + r) = r + 2 = 0$. So $r = -2$. And $u = -\frac{z-1}{z-2}$ is the only solution of the Riccati equation. Let $A = \begin{pmatrix} 0 & 1 \\ -z & -z \end{pmatrix}$ and $T_1 = \begin{pmatrix} 1-u & 1 \\ -u & 1 \end{pmatrix} = \begin{pmatrix} \frac{2z-3}{z-2} & 1 \\ \frac{z-1}{z-2} & 1 \end{pmatrix}$. Then $B_1 = \phi(T_1)AT_1^{-1} = \begin{pmatrix} -\frac{z-1}{z-2} & -\frac{z^3-6z^2+9z-3}{(z-1)(z-2)^2} \\ 0 & -\frac{z(z-2)}{z-1} \end{pmatrix}$. The entries on the diagonal of B_1 are not yet reduced. Therefore let $T_2 = \begin{pmatrix} \frac{1}{z-2} & 0 \\ 0 & z-2 \end{pmatrix}$. Then $B_2 = \phi(T_2)B_1T_2^{-1} = \begin{pmatrix} -1 & -\frac{z^3-6z^2+9z-3}{(z-1)^2(z-2)^2} \\ 0 & -z \end{pmatrix}$. Now the system $\phi(\mathbf{y}) = B_2\mathbf{y}$ is in standard form. Hence the difference Galois group is the reducible group $G = \{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \mid \alpha^2 = 1 \}$.

A fundamental matrix for system (B_2) with entries in $\mathcal{S}_{\mathbf{Q}}$ is $U_2 = \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ 0 & \mathbf{d} \end{pmatrix}$,

where $a_n = (-1)^n$, $d_n = (-1)^n(n-1)!$ and $b_n = (-1)^n\tilde{b}_n$ where the sequence $\tilde{\mathbf{b}} = (\tilde{b}_1, \tilde{b}_2, \dots)$ satisfies the inhomogeneous equation $\tilde{b}_{n+1} - \tilde{b}_n = (n-1)! \frac{n^3-6n^2+9n-3}{(n-1)^2(n-2)^2}$

for all but finitely many n . Hence we can take $\tilde{b}_n = \sum_{k=3}^{n-1} (k-1)! \frac{k^3-6k^2+9k-3}{(k-1)^2(k-2)^2}$ for all

$n \geq 3$. Now $T_1^{-1}T_2^{-1}U_2$ is a fundamental matrix for the equation $\phi^2y + z\phi y + zy = 0$. Two linearly independent solutions of this equation are $\mathbf{u}, \mathbf{v} \in \mathcal{S}_{\mathbf{Q}}$, where

$$u_n = (-1)^n(n-2) \text{ and } v_n = (-1)^n \left(-\frac{(n-1)!}{n-2} + (n-2) \sum_{k=3}^{n-1} (k-1)! \frac{k^3-6k^2+9k-3}{(k-1)^2(k-2)^2} \right).$$

Example 2. Consider the equation $\phi^2(y) - \frac{3z+14}{z+9}\phi(y) + \frac{2z}{z+9}y = 0$. We want to determine the set S_u . Let $t = \frac{1}{z}$. The Riccati equation at ∞ reads $u\phi(u) - \frac{3+14t}{1+9t}u + \frac{2}{1+9t} = 0$. We have $v(-\frac{3+14t}{1+9t}) = v(\frac{2}{1+9t}) = 0$. Hence we are in the case that $v(b) \leq 2v(a)$ and $v(b)$ is even. We find $S_u = \{1-5t+O(t^2), 2-8t+O(t^2)\}$. Further we have $S_p = \{1, z\}$ and $S_q = \{1, z+8\}$. There are four combinations $u \in S_u$, $p \in S_p$ and $q \in S_q$ such that $v(u) + v(q) - v(p) = 0$. The first two combinations are $p = 1, q = 1$ and $u = 1-5t+O(t^2)$ or $u = 2-8t+O(t^2)$. These two combinations does not yield any solution $u \in \mathbf{Q}(z)$ of the Riccati equation. The third combination is $p = z, q = z+8$ and $u = 1-5t+O(t^2)$. This combination gives us $\frac{uq}{p} = 1+3t+O(t^2)$. So $e = 3$. After substituting $c = 1, p = z, q = z+8$ and $R = z^3 + r_2z^2 + r_1z + r_0$ in $(\ddagger)$ we are left with four linear equations in the three indeterminates r_0, r_1 and r_2 . There is a unique solution $r_0 = 1680, r_1 = 392$ and $r_2 = 33$. So $R = z^3 + 33z^2 + 392z + 1680 = (z+12)(z^2+21z+140)$. The fourth combination is $p = z, q = z+8$ and $u = 2-8t+O(t^2)$. This combination gives us $\frac{uq}{2p} = 1+4t+O(t^2)$. After substituting $c = 2, p = z, q = z+8$ and $R = z^4 + r_3z^3 + r_2z^2 + r_1z + r_0$ in $(\ddagger)$ we are left with five linear equations in the four indeterminates r_0, r_1, r_2 and r_3 . There is a unique solution $r_0 = 840, r_1 = -386, r_2 = 83$ and $r_3 = -10$. So $R = z^4 - 10z^3 + 83z^2 - 386z + 840$. The solutions of the Riccati equation are $u_1 = \frac{z(z+13)(z^2+23z+162)}{(z+8)(z+12)(z^2+21z+140)}$ and $u_2 = 2\frac{z(z^4-6z^3+59z^2-246z+528)}{(z+8)(z^4-10z^3+83z^2-386z+840)}$. Let

$$T_1 = \begin{pmatrix} -\frac{u_2}{u_1-u_2} & -\frac{1}{u_1-u_2} \\ -\frac{u_1-u_2}{u_1} & -\frac{1}{u_1} \end{pmatrix}. \text{ Then } B_1 = \phi(T_1) \begin{pmatrix} 0 & 1 \\ -\frac{2z}{z+9} & \frac{3z+14}{z+9} \end{pmatrix} T_1^{-1} =$$

$$\begin{pmatrix} \frac{z(z+13)(z^2+23z+162)}{(z+8)(z+12)(z^2+21z+140)} & 0 \\ 0 & 2\frac{z(z^4-6z^3+59z^2-246z+528)}{(z+8)(z^4-10z^3+83z^2-386z+840)} \end{pmatrix}.$$

The entries on the diagonal of B_1 are not yet reduced. Therefore we apply the algorithm for first order difference equations to $\frac{z(z+13)(z^2+23z+162)}{(z+8)(z+12)(z^2+21z+140)}$ and $2\frac{z(z^4-6z^3+59z^2-246z+528)}{(z+8)(z^4-10z^3+83z^2-386z+840)}$. In this way we find a matrix

$$T_2 = \begin{pmatrix} \frac{(z+12)(z^2+21z+140)}{z(z+1)(z+2)(z+3)(z+4)(z+5)(z+6)(z+7)} & 0 \\ 0 & \frac{z^4-10z^3+83z^2-386z+840}{z(z+1)(z+2)(z+3)(z+4)(z+5)(z+6)(z+7)} \end{pmatrix}$$

such that $B_2 = \phi(T_2)B_1T_2^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. Now the system $\phi(\mathbf{y}) = B_2\mathbf{y}$ is in standard form. Hence the difference Galois group is the completely reducible group $G = \{ \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix} \mid \delta \in \bar{\mathbf{Q}}^* \}$.

A fundamental matrix for system (B_2) with entries in $\mathcal{S}_{\bar{\mathbf{Q}}}$ is $U_2 = \begin{pmatrix} \mathbf{a} & 0 \\ 0 & \mathbf{d} \end{pmatrix}$, where $a_n = 1$ and $d_n = 2^n$. Now $T_1^{-1}T_2^{-1}U_2$ is a fundamental matrix for the equation $\phi^2(y) - \frac{3z+14}{z+9}\phi(y) + \frac{2z}{z+9}y = 0$. Two linearly independent solutions of this equation are $\mathbf{u}, \mathbf{v} \in \mathcal{S}_{\bar{\mathbf{Q}}}$ where

$$u_n = \frac{(n+12)(n^2+21n+140)}{n(n+1)(n+2)(n+3)(n+4)(n+5)(n+6)(n+7)} \text{ and } v_n = \frac{n^4-10n^3+83n^2-386n+840}{n(n+1)(n+2)(n+3)(n+4)(n+5)(n+6)(n+7)} 2^n.$$

Remark. In example 1 and 2, two special cases of the so-called hypergeometric difference equations are discussed. For an extensive study of hypergeometric difference equations we refer to [Bat67].

Example 3. Now consider the equation $\phi^2y + a\phi y + by = 0$, where $a = \frac{(z+1)(5z^2+8z+4)}{(z+2)(z^5+2z^4+z^3-1)}$ and $b = -\frac{z^2(z^5+7z^4+19z^3+25z^2+16z+3)}{(z+2)(z^5+2z^4+z^3-1)}$. We have $v(a) = 3$ and $v(b) = -1$. (See Subsection 4.4.1.) Hence we are in the case that $v(b) \leq 2v(a)$ and $v(b)$ is odd. So there does not exist a rational solution of the Riccati equation. Hence the difference Galois group G is irreducible. We want to determine whether the difference Galois group is imprimitive. According to theorem 4.4.6. G is imprimitive if and only if there exists a solution E of the Riccati equation

$$\phi^2(E)E + (\phi^2(\frac{b}{a}) - \phi(a) + \frac{\phi(b)}{a})E + \frac{\phi(b)b}{a^2} = 0.$$

Here we have $\phi^2(\frac{b}{a}) - \phi(a) + \frac{\phi(b)}{a} = -\frac{(z+2)(10z^3+51z^2+88z+48)(z^5+12z^4+57z^3+134z^2+156z+71)}{(z+3)(5z^2+8z+4)(5z^2+28z+40)}$ and $\frac{\phi(b)b}{a^2} = \frac{z^2(z+2)(z^5+2z^4+z^3-1)(z^5+12z^4+57z^3+134z^2+156z+71)}{(z+3)(5z^2+8z+4)^2}$. Using the algorithm for the Riccati equation we find two solutions $E_1 = \frac{z^2(z^5+2z^4+z^3-1)}{(z+1)(5z^2+8z+4)}$ and $E_2 = \frac{(z+2)^2(z^5+2z^4+z^3-1)}{z(5z^2+8z+4)}$. Let $D = E_2 + \frac{b}{a} = -\frac{1}{z(z+1)}$ and $r = -a\phi(a) + \phi(b) + a\phi^2(D) = -\frac{z^3(z+1)(z^5+12z^4+57z^3+134z^2+156z+71)}{(z+2)^2(z+3)(z^5+2z^4+z^3-1)}$. Then y is a solution of the equation $\phi^2y + a\phi y + by = 0$. if and only if $Dy + \phi y$ satisfies $\phi^2y + ry = 0$.

We have $B_1 = \begin{pmatrix} 0 & 1 \\ -r & 0 \end{pmatrix} \phi(T_1) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T_1^{-1}$, where $T_1 = \begin{pmatrix} D & 1 \\ -b & \phi(D) - a \end{pmatrix}$.

Now $-r$ is not yet reduced. Therefore let $T_2 = \begin{pmatrix} f & 0 \\ 0 & \phi(f) \end{pmatrix}$, where $f = \frac{z^2(z+1)}{z^5+2z^4+z^3-1}$.

Then $B_2 = \phi(T_2)B_1T_2^{-1} = \begin{pmatrix} 0 & 1 \\ z & 0 \end{pmatrix}$. The system $\phi(\mathbf{y}) = B_2\mathbf{y}$ is in standard form.

Hence the difference Galois group is the imprimitive group $G = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid \alpha\delta \neq 0 \} \cup \{ \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \mid \beta\gamma \neq 0 \}$.

A fundamental matrix for system (B_2) with entries in $\mathcal{S}_{\mathbf{Q}}$ is $U_2 = \begin{pmatrix} \mathbf{c} & \mathbf{d} \\ \rho(\mathbf{c}) & \rho(\mathbf{d}) \end{pmatrix}$,

where $c_n = \prod_{k=1}^{\frac{n}{2}-1} 2k$ if n is even and $c_n = 0$ if n is odd and $d_n = \prod_{k=1}^{\frac{n-1}{2}} (2k-1)$ if n is odd and $d_n = 0$ if n is even. Now $T_1^{-1}T_2^{-1}U_2$ is a fundamental matrix for the equation $\phi^2 y + a\phi y + by = 0$. And we find two linearly independent solutions $\mathbf{u}$ and $\mathbf{v}$ of this equation, where $u_n = \frac{1}{n}c_n + nc_{n+1}$ and $v_n = \frac{1}{n}d_n + nd_{n+1}$.

4.5.2 The case where an extension of the constant field is needed

In this subsection we will construct second order difference equations, for which a quadratic field extension of the constant field is needed for solving the Riccati equation. In particular we will give an example to show that step 3 in the algorithm for solving the Riccati equation is not superfluous.

Let $\tilde{k} = k(\lambda)$ with $\lambda^2 \in k$ and $\lambda \notin k$. Take $u_0, u_1 \in k(z)$ with $u_1 \neq 0$. And let $u = u_0 + \lambda u_1$. Then $\phi(u)u + au + b = 0$ is equivalent to the equations

$$u_0\phi(u_0) + \lambda^2\phi(u_1)(u_1) + au_0 + b = 0$$

and

$$\phi(u_0)u_1 + u_0\phi(u_1) + au_1 = 0.$$

Hence a and b are uniquely determined if we fix $u_0, u_1 \in k(x)$ with $u_1 \neq 0$. Obviously $u_0 + \lambda u_1$ and $u_0 - \lambda u_1$ are two solutions of the Riccati equation associated to the difference equation $\phi^2 y + a\phi y + by = 0$. If the difference Galois group G of this equation is not an algebraic subgroup of $\{c.Id \mid c \in \bar{\mathbf{Q}}^*\}$, that is if $\frac{u_0 + \lambda u_1}{u_0 - \lambda u_1}$ is not of the form $\frac{\phi(f)}{f}$ with $f \in \tilde{k}(z)$, then $u_0 + \lambda u_1$ and $u_0 - \lambda u_1$ are the only solutions of the Riccati equation and we really need the quadratic extension $\tilde{k} \supset k$ for solving the Riccati equation.

If we take $u_0 = z^2$ and $u_1 = 1$ then we get the second order equation $\phi^2 + (-2z^2 - 2z - 1)\phi y + (z^4 - \lambda^2)y = 0$. Clearly in this case we do not need a quadratic extension of our constant field k for computing the first two terms of the local formal solution at infinity of the associated Riccati equation. Furthermore $\frac{u_0 + \lambda u_1}{u_0 - \lambda u_1}$ is not of the form $\frac{\phi(f)}{f}$ with $f \in k(z)$. Hence we need step 3 of the algorithm described in section 4.4.1 in order to find the quadratic field extension $\tilde{k}$ needed for solving the Riccati equation.

Two linearly independent solutions in $\mathcal{S}_{\mathbf{Q}}$ of this second order difference equation are $\mathbf{c}, \mathbf{d}$, where $c_n = \prod_{j=1}^{n-1} (j^2 + \lambda)$ and $d_n = \prod_{j=1}^{n-1} (j^2 - \lambda)$. If one wants to have a basis consisting of two k -rational solutions then one can take $\frac{1}{2}(\mathbf{c} + \mathbf{d})$ and $\frac{1}{2\lambda}(\mathbf{c} - \mathbf{d})$.

Chapter 5

An algorithm for computing a standard form for second order linear q -difference equations

5.1 Introduction

In this article we will present an algorithm for computing a standard form for second order q -difference equations over the rational function field $k(z)$, where k denotes a finite algebraic extension of $\mathbf{Q}(q)$ and z is a transcendental variable. This standard form will be defined in section 5.2. One can read off fairly easily the q -difference Galois group of a system of q -difference equations if one knows that the system is in standard form. Moreover, if the q -difference Galois group of a second order q -difference equation is not too big (i.e. does not contain $Sl(2, \mathbf{C})$) then one can compute two linearly independent Liouvillian solutions for this equation. For analogous algorithms for second order differential equations and second order difference equations we refer to [Kov86] and [Hen96] respectively.

In section 5.2 a standard form for q -difference equations will be defined. Further some notation will be fixed. In section 5.3 we will discuss first order homogeneous linear q -difference equations. The algorithm for second order homogeneous q -difference equations will be explained in section 5.4. Section 5.5 is devoted to examples.

5.2 A short introduction to algebraic aspects of q -difference equations.

We will use the following notation.

- $q \in \mathbf{C}$, but q is not a root of unity and $q \neq 0$.

- $q_1, q_2, q_3, \dots$ is a sequence of complex numbers satisfying $q_1 = q$ and $q_{i+1}^{i+1} = q_i$.
- We define recursively $K_1 = \mathbf{C}(z_1)$ and $K_{i+1} = \mathbf{C}(z_{i+1})$, where $z_{i+1}^{i+1} = z_i$. Instead of K_1 and z_1 we will write K and z .
- $K_\infty = \bigcup_{i=1}^{\infty} K_i$.
- ϕ denotes the $\mathbf{C}$ -linear automorphism of K_∞ given by $\phi(z_i) = q_i z_i$. Obviously ϕ can be restricted to the fields K_i . We will denote these restrictions also by ϕ .

We are interested in the Galois theory of q -difference equations over the field K_∞ , because if one works over this field there is a standard form available analogous to the standard form which is defined for ordinary difference equations in [Hen96]. This is not the case if one works over the smaller field $K = \mathbf{C}(z)$. Consider the system of difference equations (A) : $\phi \mathbf{y} = A \mathbf{y}$, where $A \in Gl(n, K_\infty)$. (We restrict ourselves to equations with $A \in Gl(n, K_\infty)$ in order to guarantee that we get n independent solutions.)

Definition 5.2.1 *A ring R together with an automorphism $\phi_R : R \rightarrow R$ is called a Picard-Vessiot extension over K_∞ associated with system (A) if*

1. R is a commutative ring, $R \supseteq K_\infty$ and $\phi_R|_{K_\infty} = \phi$.
2. The only ϕ_R -invariant ideals are 0 and R .
3. There exists a matrix $U \in Gl(n, R)$ such that $\phi_R(U) = AU$. (Such a matrix U is called a fundamental matrix for the system (A).)
4. R is minimal with respect to the conditions 1, 2 and 3 or equivalently if $U = (u_{ij}) \in Gl(n, R)$ is a fundamental matrix for the system (A) then $R = K_\infty[u_{11}, \dots, u_{nn}, \frac{1}{\det(U)}]$.

From now on we will denote ϕ_R also by ϕ .

Theorem 5.2.2 *(Existence and unicity) For every system of linear q -difference equations (A) with $A \in Gl(n, K_\infty)$ there exist a Picard-Vessiot extension $R \supseteq K_\infty$. This extension is unique up to q -difference K_∞ -isomorphism, that is up to K_∞ -linear isomorphisms commuting with ϕ . Further we have that $\phi(r) = r$ implies $r \in \mathbf{C}$ if $r \in R$.*

Definition 5.2.3 *The q -difference Galois group $G = DGal(R/K_\infty)$ is the group consisting of all the q -difference K_∞ -automorphisms of R .*

The vector space of solutions V is the set $\{\mathbf{y} \in R^n \mid \phi(\mathbf{y}) = A\mathbf{y}\}$. If $U \in GL(n, R)$ is a fundamental matrices for the system (A) then the columns of U form a base for V over $\mathbf{C}$. Suppose that $\sigma \in G = DGal(R/K_\infty)$, then it is obvious that $\sigma(U)$ is also a fundamental matrix for the sytem (A). Hence $\sigma(U) = UT_\sigma$, where $T_\sigma, T_{\sigma_\infty} \in Gl(n, \mathbf{C})$. So the elements of the q -difference Galois groups act as $\mathbf{C}$ -linear maps on the $\mathbf{C}$ -linear space of solutions V . But even a stronger statement holds.

Theorem 5.2.4 (*Algebraicity*) $G = DGal(R/K_\infty)$ is a linear algebraic groups over the field of constants $\mathbf{C}$.

Theorem 5.2.5 (*Galois correspondence*)

1. If $a \in R$ then $(\forall \sigma \in G : \sigma(a) = a) \Rightarrow a \in K_\infty$.
2. If H is an algebraic subgroup of G such that $K_\infty = \{a \in R \mid \forall \sigma \in H : \sigma(a) = a\}$ then $H = G$.

Theorems 5.2.2, 5.2.4 and 5.2.5 are special cases of theorems for more general difference fields which are proved in chapter 1 of [PS96].

If G is an algebraic subgroup of $Gl(n, \mathbf{C})$, then we denote by $G(K_\infty)$ the subgroup of $Gl(n, K_\infty)$ which is defined by the same equations. Two systems (A) and (B) corresponding to matrices $A, B \in Gl(n, K_\infty)$ are defined to be equivalent over K_∞ if there exists a $T \in Gl(n, K_\infty)$ such that $B = \phi(T)AT^{-1}$. In this case, if $U \in Gl(n, R)$ is a fundamental matrix of system (A) then TU is a fundamental matrix of system (B) and it is obvious that the solution spaces V_A, V_B of the systems (A) and (B) are equivalent as representation spaces of the q -difference Galois group G . Conversely if the Picard-Vessiot extensions associated to the systems (A) and (B) are q -difference K_∞ -isomorphic and the solution spaces V_A and V_B are equivalent as representation spaces of the q -difference Galois group G then (A) and (B) are equivalent systems of q -difference equations.

The algorithms in section 3 and section 4 are based on theorem 5.2.6 and the converse theorem 5.2.7. These theorems are not valid for general difference fields.

Theorem 5.2.6 Let $G \subseteq Gl(n, \mathbf{C})$ be the q -difference Galois group associated to the system of difference equations (A). Then the following statements hold.

1. G/G^0 is a finite cyclic group.
2. There exists a $B \in G(K_\infty)$ such that (A) and (B) are equivalent systems.

It is a conjecture that for every linear algebraic group $G \subseteq Gl(n, \mathbf{C})$ with G/G^0 finite cyclic there exists a system of difference equations which has G as difference Galois group. One can show that this conjecture is true for $n = 1, 2$ by giving explicit examples for every possible group.

Theorem 5.2.7 *If $A \in G(K_\infty)$ with G an algebraic subgroup of $GL(n, \mathbf{C})$ such that for any proper algebraic subgroup H and for any $T \in G(K_\infty)$ one has that $\phi(T)AT^{-1} \notin H(K_\infty)$ then G is the difference Galois group of the system (A) .*

Definition 5.2.8 *If A satisfies the conditions of theorem 5.2.7 then we say that system (A) is in standard form.*

This standard form is in general not unique. But one can read off fairly easily the q -difference Galois group of a system of q -difference equations if one knows already that this system is in standard form. The standard form is also very suitable for finding Liouvillian solutions. This will be explained in section 5.5. In fact we will present an algorithm which computes for a given equation an equivalent system in standard form.

The proofs of theorems 5.2.6 and 5.2.7 are completely analogous to the proofs of propositions 1.20 and 1.21 in [PS95] if one applies the next two lemmas.

Lemma 5.2.9 *K_∞ is a quasi-algebraically closed (or C_1) field.*

Proof. A field L is called quasi-algebraically closed if it satisfies the condition that if P is a homogeneous polynomial of degree $d \neq 0$ in n variables with coefficients in L whose only zero in L^n is $(0, \dots, 0)$, then $d \geq n$. Let P be a homogeneous polynomial of degree $d \neq 0$ in n variables with coefficients in K_∞ . Assume that $(0, \dots, 0)$ is the only zero of P in K_∞^n . There exists an $m \in \mathbf{Z}_{\geq 1}$ such that the coefficients of P are in K_m . The fields K_i are extensions of transcendence degree 1 of an algebraically closed field. Such fields are well known to be quasi-algebraically closed. Hence $d \geq n$. $\square$

A consequence of lemma 5.2.9 is that if G is a connected group then

$$H^1(\text{Gal}(\bar{K}_\infty/K_\infty), G(\bar{K}_\infty)) = 0$$

, where $\bar{K}_\infty$ denotes the algebraic closure of K_∞ . See [Ser64].

Lemma 5.2.10 *The automorphism ϕ does not extend to any proper finite extension L of K_∞ .*

Proof. Suppose L is a finite algebraic extension of K_∞ . Then $L = K_\infty(\alpha)$ for a certain $\alpha \in L$. The coefficients of the monic irreducible polynomial for α over K_∞ are in K_m for an $m \in \mathbf{Z}$. Let ρ denote the morphism of algebraic curves $X \rightarrow \mathbf{P}(\mathbf{C})$ corresponding to $K_m(\alpha) \supset K_m$. If ϕ extends to $K_m(\alpha)$ then ϕ will permute the finite ramification points of ρ . The automorphism ϕ of $\mathbf{P}(\mathbf{C})$ leaves no finite subset of $\mathbf{P}(\mathbf{C})$ invariant. This implies that ρ is a finite cyclic covering whose only ramification points are 0 and ∞ . Hence $K_m(\alpha) \subset K_\infty$. $\square$

The equations that we look at in the next sections are defined over a small field $k(z) \subset \mathbf{C}(z)$, where k denotes a finite algebraic extension of $\mathbf{Q}(q)$. The algorithm works in the field K_∞ , but in reality we will use only a small part of this field. In the main part of the algorithm (section 5.4.1) it suffices to work over fields $l(z_2)$, where $l \subset \mathbf{C}$ is a degree 2 extension of k .

5.3 First order q -difference equations

We consider the first order homogeneous linear difference equation $(a) : \phi y = ay$ with $a \in k(z)^*$, where k is a finite algebraic extension of $\mathbf{Q}(q)$. Any equivalent equation is given by $\phi y = \frac{\phi(f)}{f} ay$, where $f \in K_\infty^*$. The q -difference Galois group G of (a) is a finite cyclic group of order n if there is a $f \in K_\infty^*$ such that $\frac{\phi(f)}{f}a$ is a primitive n^{th} -root of unity, otherwise the difference Galois group is the multiplicative group $\mathbf{G}_m = \mathbf{C}^*$. This statement is a consequence of Theorems 5.2.6 and 5.2.7.

Suppose $a \in k(z)^*$. Then we can write $a = cz^m \frac{P}{Q}$, where $c \in k$, $m \in \mathbf{Z}$ and $P, Q \in k[z]$ are monic polynomials with $\gcd(P, Q) = \gcd(P, z) = \gcd(Q, z) = 1$. Notice that c, m, P, Q are uniquely determined by a .

Definition 5.3.1 Suppose that $a = cz^m \frac{P}{Q} \in k(z)^*$. Then a is reduced if

1. For all $n \in \mathbf{Z}$ we have $\gcd(P, \phi^n Q) = 1$.
2. If $c = q^r \omega$ where $r \in \mathbf{Q}$ and ω is a root of unity then $r = 0$.

If a is reduced then the equation $(a) : \phi(y) = ay$ is automatically in standard form.

Suppose $a \in K$ is given. We describe an algorithm which produces an element $b \in K$ such that the difference equations (a) and $(b) : \phi(y) = by$ are equivalent and b is reduced.

We assume that $a = cz^m \frac{P}{Q}$, where $c \in k$, $m \in \mathbf{Z}$ and $P, Q \in k[z]$ are monic polynomials with $\gcd(P, Q) = \gcd(P, z) = \gcd(Q, z) = 1$. If $c = q^r \omega$ where $r \in \mathbf{Q}$ and ω is a root of unity then we replace c by $\omega = \frac{\phi(z^{-r})}{z^{-r}} c$.

Write $P = P_1 P_2 \cdots P_s$ and $Q = Q_1 Q_2 \cdots Q_t$ where the P_i and Q_j are monic and irreducible in $k[z]$. First we take P_1 and we test whether there exist a Q_j and an $n \in \mathbf{Z}$ such that $\phi^n P_1 = Q_j$. If $\phi^n P_1 = Q_j$ then we can go further with $\tilde{a} = a \frac{Q_j}{P_1}$. This gives a reduction of the problem with respect to the number of irreducible factors of P and Q . And then we proceed with $\tilde{a}$ instead of a and so forth.

There is also an algorithm which avoids factorization in $k[z]$ if $|q| \neq 1$. We will present this algorithm here. If $|q| \neq 1$ there exists an $R > 0$ such that the zeros of P and Q are in the annulus $\frac{1}{R} \leq |z| \leq R$. We can express R in terms of the coefficients of P and Q . For instance if $P = P_c z^c + \cdots + P_1 z + P_0$ and $Q = Q_d z^d +$

$\cdots + Q_1 z + Q_0$ then we can take $R = 1 + \max(\sum_{i=0}^{c-1} \frac{|P_i|}{|P_c|}, \sum_{j=0}^{d-1} \frac{|Q_j|}{|Q_d|}, \sum_{i=1}^c \frac{|P_i|}{|P_0|}, \sum_{j=1}^d \frac{|Q_j|}{|Q_0|})$.

For $m \in \mathbf{Z}$ with $|q^m| > R^2$ or $|q^m| < \frac{1}{R^2}$ we have $\gcd(P, \phi^m Q) = 1$. We start with $m = 1$ and compute $g = \gcd(P, \phi(Q))$. If $g \neq 1$ then one can write $a = \frac{g}{\phi^{-1}(g)} \frac{\tilde{P}}{\tilde{Q}}$ and we can go further with $\tilde{a} = \frac{\tilde{P}}{\tilde{Q}}$ instead of a . This gives a reduction of the problem with respect to the degrees of P and Q . If $g = 1$ then we try $m = -1$ and so forth. The algorithm stops if a is reduced to a constant or if all $m \in \mathbf{Z}$ with $\frac{1}{R^2} \leq |q^m| \leq R^2$ are checked off.

The above algorithms can easily be modified so that we also find an $f \in K_\infty$ that $b = \frac{\phi(f)}{f} a$ is reduced.

5.4 Second order q -difference equations

Consider the second order linear homogeneous q -difference equation $\phi^2 y + a\phi y + by = 0$, where $a, b \in k(z)$ and $b \neq 0$. As usual we will identify this equation with the 2×2 system of q -difference equations $(A) : \phi \mathbf{y} = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \mathbf{y}$. Throughout this section we will denote the q -difference Galois group over K_∞ of above system by G .

We present an algorithm which produces a matrix $B \in Gl(2, K_\infty)$ so that the systems (A) and (B) are equivalent and (B) is in standard form. Further a matrix T is computed such that $B = \phi(T)AT^{-1}$.

Lemma 5.4.1 *The algebraic subgroups G of $Gl(2, \mathbf{C})$ that can occur as q -difference Galois group over K_∞ are*

1. *Any reducible subgroup of $Gl(2, \mathbf{C})$ with G/G^0 finite cyclic.*
2. *Any infinite imprimitive subgroup of $Gl(2, \mathbf{C})$ with G/G^0 finite cyclic.*
3. *Any subgroup containing the group $Sl(2, \mathbf{C})$.*

Proof. This is a consequence of theorem 5.2.6. and the well known classification of the algebraic subgroups of $Gl(2, \mathbf{C})$. $\square$

The algorithm is arranged in the following manner. Given a second order q -difference equation we test which of the three cases above holds. After that we compute an appropriate equivalent system in standard form.

5.4.1 The Riccati equation

To a second order linear q -difference equation $\phi^2 y + a\phi y + by = 0$, where $a, b \in k(z)$ and $b \neq 0$ we can associate a first order non-linear q -difference equation $(\dagger) : u\phi(u) + au + b = 0$. This equation is called the Riccati equation. If u is a solution of the Riccati equation then the q -difference operator $\phi^2 + a\phi + b$ factors

as $(\phi - \frac{b}{u})(\phi - u)$. A solution in K_∞ of the Riccati equation corresponds to a line of the solution space that is fixed by the q -difference Galois group G . Therefore we have the following theorem. See also [Hen96].

Theorem 5.4.2 *The following statements hold:*

1. *If the Riccati equation has no solutions $u \in K_\infty^*$ then G is irreducible.*
2. *If the Riccati equation has exactly one solution $u \in K_\infty^*$ then G is reducible but not completely reducible.*
3. *If the Riccati equation has exactly two solutions $u_1, u_2 \in K_\infty^*$ then G is completely reducible but G is not an algebraic subgroup of $\{c.Id \mid c \in \mathbf{C}^*\}$.*
4. *If the Riccati equation has more than two solutions in K_∞^* then the Riccati equation has infinitely many solutions and G is an algebraic subgroup of $\{c.Id \mid c \in \mathbf{C}^*\}$.*

In this section we will describe an algorithm which computes all solutions $u \in K_\infty^*$ of the Riccati equation. The algorithm consists of a few steps. In the first three steps we will compute all solutions $u \in K$ of the Riccati equation. In the first step of the algorithm we will compute the first term of all possible local formal solutions at 0 and ∞ . In the next two steps we try to glue these local formal solutions to a global solution. In the fourth step we will prove that if there exists a solution $u \in K_\infty$ then there is also a solution $u \in K_2$. After that we will describe how to find the solutions $u \in K_2$ if we did not find any solution $u \in K$.

1. Let ϕ be the automorphism of $\mathbf{C}((z))$ given by $\phi(z) = qz$. Then ϕ coincides with our former ϕ on $K = \mathbf{C}(z)$.

We define the discrete valuation $v_0 : \mathbf{C}((z)) \rightarrow \mathbf{Z}$ by $v_0(\sum_{i=-\infty}^{\infty} c_i z^i) = \min\{i \mid c_i \neq 0\}$. In particular $v_0(0) = \infty$. Elementary properties of v_0 are $v_0(u_1 u_2) = v_0(u_1) + v_0(u_2)$ and $v_0(u_1 + u_2) \geq \min(v_0(u_1), v_0(u_2))$. Hence if $v_0(u_1) \neq v_0(u_2)$ then $v_0(u_1 + u_2) = \min(v_0(u_1), v_0(u_2))$. Another property of v_0 is that $v_0(u) = v_0(\phi u)$. Now we consider a and b as Laurent series in z .

We distinguish two cases.

- (a) $2v_0(a) < v_0(b)$. In this case there are two solutions $u, \tilde{u} \in k((z))$ of the Riccati equation. The first solution u satisfies $v_0(au) = v_0(u\phi(u)) < v_0(b)$ and $v_0(u) = v_0(a)$ and the other solution $\tilde{u}$ satisfies $v_0(a\tilde{u}) = v_0(b) < v_0(\tilde{u}\phi(\tilde{u}))$ and $v_0(\tilde{u}) = v_0(b) - v_0(a)$. Suppose $v_0(a) = l$ and $v_0(b) = k$. Then we will write $a = \sum_{i=l}^{\infty} a_i z^i$ and $b = \sum_{i=k}^{\infty} b_i z^i$. We can compute successively the coefficients of u and $\tilde{u}$ by simply solving

linear equations with coefficients in k . Hence no field extension of k is needed. We find $u = -\frac{a_l}{q^l}z^l + O(z^{l+1})$, where $O(z^{l+1})$ stands for the higher order terms and $\tilde{u} = -\frac{b_k}{a_l}z^{k-l} + O(z^{k-l+1})$.

- (b) $v_0(b) \leq 2v_0(a)$. If $u \in \mathbf{C}((z))$ satisfies the Riccati equation then we have $v_0(b) = v_0(u\phi(u)) \leq v_0(au)$. Hence if $v_0(b)$ is odd there is obviously no solution of the Riccati equation in the field $\mathbf{C}((z))$. Suppose now $v_0(b)$ is even. Let $n = \frac{1}{2}v_0(b)$. Write $b = \sum_{i=2n}^{\infty} b_i z^i$ and $a = \sum_{i=n}^{\infty} a_i z^i$. (Note that it is possible that $a_n = 0$). Write $u = \sum_{i=n}^{\infty} b_i z^i$. Then we try to solve the Riccati equation $(\dagger) : u\phi(u) + au + b = 0$. The $(2n)^{th}$ -coefficient of this expression gives us the equation $q^n u_n^2 + a_n u_n + b_{2n} = 0$. Let $D_0 = a_n^2 - 4b_{2n}q^n$. If $D_0 \neq 0$ then we find two solutions $u_n = \frac{-a_n \pm \sqrt{D_0}}{2q^n} \in k(\sqrt{D_0})$ of the quadratic equation. So $u = \frac{-a_n \pm \sqrt{D_0}}{2q^n} z^n + O(z^{n+1})$. If $D_0 = 0$ then we find one solution $u = \frac{-a_n}{2q^n} z^n + O(z^{n+1})$.

Let S_0 be the set of all possibilities for the first term of u expressed as Laurent series in z . The coefficient of this term lies in the field $k(\sqrt{D_0})$ with $[k(\sqrt{D_0}) : k] \leq 2$. We discovered that $\#S_0 \leq 2$, even if the Riccati equation has infinitely many solutions $u \in K_{\infty}$. In the same way we can determine the set S_{∞} of all possibilities for the first term of u expressed as Laurent series in $\frac{1}{z}$ with a coefficient in at worst a quadratic field extension $k(\sqrt{D_{\infty}})$. We also have $\#S_{\infty} \leq 2$. For future use we will denote $\tilde{k} = k(\sqrt{D_0}, \sqrt{D_{\infty}})$.

2. In this part of the algorithm we will determine the solutions $u \in \tilde{k}(z)$ of the Riccati equation. We rewrite the Riccati equation as $Fu\phi(u) + Gu + H = 0$, where $F, G, H \in k[z]$ and $\gcd(F, G, H) = 1$. Write $u = cz^m \frac{P}{T}$ with $c \in \tilde{k}$, $m \in \mathbf{Z}$, $P, T \in \tilde{k}[z]$, where P and T are monic polynomials and $\gcd(P, T) = \gcd(P, z) = \gcd(T, z) = 1$. Let R denote the greatest monic divisor of T such that $\phi(R)$ divides P . Then one can write $u = cz^m \frac{\phi(R)p}{Rt}$, where p, t are monic polynomials, $\gcd(p, \phi(t)) = 1$ and $\gcd(\phi(R)p, Rt) = 1$. Further $\gcd(R, z) = \gcd(p, z) = \gcd(t, z) = 1$. The Riccati equation reads now:

$$(\ddagger) : c^2 q^m z^{2m} \phi^2(R) \phi(p) p F + cz^m \phi(R) \phi(t) p G + R \phi(t) t H = 0.$$

Hence p is a monic divisor of H with $v_0(p) = 0$ and t is a monic divisor of $\phi^{-1}(F)$ with $v_0(t) = 0$. We define the sets $S_p = \{p \in \tilde{k}[z] \mid p|H, v_0(p) = 0 \text{ and } p \text{ monic}\}$ and $S_t = \{t \in \tilde{k}[z] \mid t|\phi^{-1}(F), v_0(t) = 0 \text{ and } t \text{ monic}\}$.

Writing $\frac{\phi(R)}{R}$ as a Laurent series in z we get $\frac{\phi(R)}{R} = 1 + O(z)$, where $O(z)$ stands for the higher order terms. $\frac{\phi(R)}{R}$ must be equal to $\frac{ut}{cz^m p}$. Hence for

every possible combination $u_0 \in S_0$, $p \in S_p$ and $t \in S_t$ we compute a $c \in \tilde{k}$ and a $m \in \mathbf{Z}$ from the equation $\frac{u_0 t}{c z^m p} = 1 + O(z)$. Let e be the degree of R . Writing $\frac{\phi(R)}{R}$ as a Laurent serie in $\frac{1}{z}$ we get $\frac{\phi(R)}{R} = q^e + O(\frac{1}{z})$. So we must have $v_\infty(u) - \deg_z(t) + m + \deg_z(p) = 0$. Hence if there are no terms $u_\infty \in S_\infty$ with $v_\infty(u_\infty) = \deg_z(t) - \deg_z(p) - m$ then there is no solution $u \in K$. For all $u_\infty \in S_\infty$ satisfying $v_\infty(u_\infty) = \deg_z(t) - \deg_z(p) - m$ we compute a $d \in \tilde{k}$ from $\frac{u_\infty t}{c z^m p} = d + O(\frac{1}{z})$. If $d = q^e$ with $e \in \mathbf{Z}_{\geq 0}$ then we write $R = z^e + r_{e-1} + \dots + r_1 z + r_0$ with indeterminates $r_0, r_1, \dots, r_{e-1}$. After substituting this R in $(\ddagger)$ we are left with a set of equations in the r_i . In this way we will find all possible solutions $u \in \tilde{k}(z)$ of the Riccati equation.

3. In step 2 we have determined all solutions $u \in \tilde{k}(z)$ of the Riccati equation. Now we have to face the problem whether it is possible that there exist solutions $u \in \bar{K}$ if there are no solutions $u \in \tilde{k}(z)$. A priori this is possible because $\phi^{-1}F$ and G need not split in linear factors in $\tilde{k}[z]$. But it is also clear from the construction in step 2 that if the Riccati equation has a solution in $\bar{K}$, there is also a solution in $l(z)$, where $l \supseteq \tilde{k}$ is the smallest field which contains the splitting fields of $\phi^{-1}F$ and G . But we have even a stronger rationality result.

Theorem 5.4.3 *If the Riccati equation has a solution in $\bar{K}$ then there is also a solution in a field $\check{k}(z)$ with $[\check{k} : k] \leq 2$.*

Proof. This proof is completely analogous to the proof of theorem 4.3. in [Hen96]. $\square$

So we want to determine all fields $\check{k} \subset l$ with $[\check{k} : k] \leq 2$. If q is algebraic then $\check{k}$ must be of the form $k(\sqrt{s})$, where s is an algebraic integer in l . Recall that l is the splitting field of the polynomial FG . After a suitable linear substitution $z \mapsto \frac{z}{n}$, where $n \in \mathbf{Z}_{\geq 1}$ we can assume that FG is monic and that the coefficients of FG are algebraic integers. s must be a divisor of the discriminant of this polynomial. This gives us a finite set of possible quadratic extensions $k(\sqrt{s})$ of k in l . If q is transcendental then $\check{k}$ must be of the form $k(\sqrt{s})$ where s is a polynomial in q_i for a certain i with algebraic integer coefficients. After a suitable linear substitution we can assume that FG is monic and the coefficients of FG are polynomials in q_i (Choose i minimal.) with algebraic integer coefficients. Now s must be a divisor of the discriminant of the polynomial FG which is a polynomial in q_i with algebraic integer coefficients. Again this gives us a finite set of possible quadratic extensions $k(\sqrt{s})$ of k in l .

For each possible quadratic extension $\check{k}$ we determine the sets $S_p = \{p \in \check{k}[z] \mid p|H, v_0(p) = 0 \text{ and } p \text{ monic}\}$ and $S_t = \{t \in \check{k}[z] \mid t|\phi^{-1}(F), v_0(t) = 0 \text{ and } t \text{ monic}\}$. After that we proceed as in 2.

4. In steps 1, 2 and 3 we have determined all solutions $u \in K = \mathbf{C}(z)$ of the Riccati equation. If we did not find any solution $u \in K$ then we try to find solutions $u \in K_\infty \setminus K$. We need the following theorem.

Theorem 5.4.4 *If the Riccati equation has a solution in K_∞^* then there is also a solution in K_2^* .*

Proof. Let U be the set of solutions of the Riccati equation in K_∞^* . The group $\text{Gal}(K_\infty^*/K)$ acts on the set U . If $\#U = 1$, say $U = \{u\}$, then u is invariant under $\text{Gal}(K_\infty^*/K)$. Hence $u \in K^*$. If $\#U = 2$, then the kernel of the map $\text{Gal}(K_\infty^*/K) \rightarrow \text{Aut}(U)$ is a subgroup of index ≤ 2 . Hence u is an element of K_2 , because K_2 is the only quadratic field extension of K in K_∞ . Suppose that $\#U = \infty$. According to theorems 5.4.2.4 and 5.2.6 there exists a $T \in \text{Gl}(2, K_\infty)$ such that $\phi(T) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T^{-1} = \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix}$ for some $u \in K_\infty$. There is a $l \in \mathbf{Z}$ such that $T \in \text{Gl}(2, K_l)$ and $u \in K_l$. Suppose $\sigma \in \text{Gal}(K_l/K)$ then $\phi(\sigma(T)) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} (\sigma(T))^{-1} = \begin{pmatrix} \sigma(u) & 0 \\ 0 & \sigma(u) \end{pmatrix}$. Hence there is a $g_\sigma \in K_l$ such that $\sigma(u) = \frac{\phi(g_\sigma)}{g_\sigma} u$. This g_σ is uniquely determined if we require that the numerator and denominator of g_σ are monic. The map $\sigma \mapsto g_\sigma$ is a 1-cocycle. Hilbert 90 states that this 1-cocycle is trivial. See [Ser68]. We can replace u by $\tilde{u} = \frac{\phi(h)}{h} u$ for a certain $h \in K_l^*$ such that $\tilde{u}$ is invariant under $\text{Gal}(K_l/K)$. Hence $\tilde{u} \in K$. Let $T_1 = hT$. Then $\phi(T_1) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T_1^{-1} = \begin{pmatrix} \tilde{u} & 0 \\ 0 & \tilde{u} \end{pmatrix}$. We have $C^{-1}T_1 \in \text{Gl}(2, K_\infty)$ satisfies $\phi(C^{-1}T_1) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} (C^{-1}T_1)^{-1} = \begin{pmatrix} \tilde{u} & 0 \\ 0 & \tilde{u} \end{pmatrix}$ if and only if $\phi(C) = C$, that is $C \in \text{Gl}(2, \mathbf{C})$. For $\sigma \in \text{Gal}(K_l/K)$ one has therefore $\sigma(T_1) = C_\sigma^{-1}T_1$ for some $C_\sigma \in \text{Gl}(2, \mathbf{C})$. The map $\sigma \mapsto C_\sigma$ is a homomorphism $\text{Gal}(K_l/K) \rightarrow \text{Gl}(2, \mathbf{C})$. We have $\text{Gal}(K_l/K)$ is a finite cyclic group. So there exists an M in $\text{Gl}(2, \mathbf{C})$ such that $M^{-1}C_\sigma M$ is a diagonal matrix for all $\sigma \in \text{Gal}(K_l/K)$. Let $T_2 = M^{-1}T_1 = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}$. Then $-\frac{t_{21}}{t_{22}}$ and $-\frac{t_{11}}{t_{12}}$ satisfy the Riccati equation. Moreover $-\frac{t_{21}}{t_{22}}$ and $-\frac{t_{11}}{t_{12}}$ are fixed by $\text{Gal}(K_l/K)$ and therefore $-\frac{t_{21}}{t_{22}}, -\frac{t_{11}}{t_{12}} \in K$. $\square$

Now we consider a, b as elements of $k(z_2)$. We apply steps 1, 2 and 3 of the algorithm with z_2 and q_2 in the role of z and q respectively. In this way we will find all solutions $u \in K_2$ of the Riccati equation. This finishes the algorithm.

5.4.2 G is reducible

If the Riccati equation has a solution in K_∞ , then the q -difference Galois group G is reducible. According to Theorem 5.2.6 we can compute an equivalent system $(A) : \phi \mathbf{y} = A \mathbf{y}$, where A has the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Moreover we can assume that $b = 0$ if the Riccati equation has two or infinitely many solutions. We denote by U the subgroup of $Gl(2, \mathbf{C})$ consisting of upper triangular matrices and by D the subgroup of diagonal matrices.

Lemma 5.4.5 *The reducible subgroups $G \subset Gl(2, \mathbf{C})$ with G/G^0 finite cyclic are*

1. *The zero-dimensional groups*

$$D_{k,l,e} = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in D \mid \alpha^k = 1, \delta^l = 1, \alpha^{eg_\alpha} \delta^{g_\delta} = 1 \}$$

and the one-dimensional groups

$$U_{k,l,e} = \{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in U \mid \alpha^k = 1, \delta^l = 1, \alpha^{eg_\alpha} \delta^{g_\delta} = 1 \}$$

for $l, k, e \in \mathbf{Z}_{\geq 1}$ with $\gcd(k, l, e) = 1$, where $g_\alpha = \frac{k}{\gcd(k, l)}$ and $g_\delta = \frac{l}{\gcd(k, l)}$.

2. *The one-dimensional groups*

$$D_{m,n} = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \in D \mid \alpha^n \delta^m = 1 \}$$

and the two-dimensional groups

$$U_{m,n} = \{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \in U \mid \alpha^n \delta^m = 1 \}$$

for $m, n \in \mathbf{Z}$

3. *The two-dimensional group D and the three-dimensional group U .*

Proof. See [Hen96]. $\square$

The algorithm continues as follows. Suppose the Riccati equation has exactly one solution in K_∞ . Then the difference Galois group G is reducible but not completely reducible. If G is a proper subgroup of U , then according to Theorem 5.2.7 there must be a matrix $T = \begin{pmatrix} f & g \\ 0 & h \end{pmatrix} \in U(K_\infty)$ such that $B = \phi(T)AT^{-1} = \begin{pmatrix} a \frac{\phi(f)}{f} & * \\ 0 & d \frac{\phi(h)}{h} \end{pmatrix} \in G_\infty(K_\infty)$.

First we want to determine whether the q -difference Galois group G is one of the one-dimensional groups described in part 1 of Lemma 5.4.4. We apply the algorithm for first order q -difference equations to a and d . This yields a new equivalent system $\tilde{A} = \begin{pmatrix} \tilde{a} & * \\ 0 & \tilde{d} \end{pmatrix}$, where $\tilde{a}$ and $\tilde{d}$ are reduced.

Suppose first that $\tilde{a}$ and $\tilde{d}$ are constant. Then the system $\tilde{A}$ is already in standard form if $\tilde{a}$ or $\tilde{d}$ is a root of unity. If both $\tilde{a}$ and $\tilde{d}$ are roots of unity, then the difference Galois group is one of the groups $U_{k,l,e}$. The q -difference Galois group G is equal to $U_{m,0}$, if $\tilde{a}$ is a primitive m -th root of unity and $\tilde{d}$ is not a root a unity. And the q -difference Galois group G is equal to $U_{0,n}$, if $\tilde{d}$ is a primitive n -th root of unity and $\tilde{a}$ is not a root a unity. If $\tilde{a}$ and $\tilde{d}$ are constant but not roots of unity then if there exist $n, m \in \mathbf{Z}$ such that $\tilde{a}^m \tilde{d}^n = q^r$ with $r \in \mathbf{Q}$ the q -difference Galois group G is one of the groups described in part 2 of lemma 5.4.4. Moreover, suppose that m is minimal and positive. In that case G is equal to the group $U_{m,n}$. If $r = 0$ then the system is already in standard form. Suppose now that $r \neq 0$. It is obvious that there exists an $f \in K_\infty$ such that $(\frac{\phi(f)}{f})^n = q^{-r}$. Let $T = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}$. Then $B = \phi(T)\tilde{A}T^{-1}$ is in standard form.

Suppose now that that $\tilde{a}$ and $\tilde{d}$ are not constant. Then the q -difference Galois group is not a group described in part 1 of Lemma 5.4.4.

If $\tilde{a}$ is constant and reduced and $\tilde{d}$ is not constant and reduced then the system $(\tilde{A})$ is already in standard form. The q -difference Galois group G is the group $U_{m,0}$, if $\tilde{a}$ is an m -th primitive root of unity. Otherwise the q -difference Galois group G is the group U .

If $\tilde{d}$ is constant and reduced and $\tilde{a}$ is not constant and reduced then the system $(\tilde{A})$ is also already in standard form. The q -difference Galois group G is the group $U_{0,n}$, if $\tilde{d}$ is an n -th primitive root of unity. Otherwise the q -difference Galois group G is the group U .

Suppose now that both $\tilde{a}$ and $\tilde{d}$ are reduced but not constant. The q -difference Galois group is one of the groups $U_{m,n}$ if and only if there exists $r, s \in \mathbf{Z} \setminus \{0\}$ with $\gcd(r, s) = 1$ and an $f \in K_\infty$ such that $\tilde{a}^r \tilde{d}^s \frac{\phi(f)}{f}$ is a root of unity. Without loss of generality we can assume that $r > 0$. Let N_a and N_d denote the degree of the numerator of $\tilde{a}$ and $\tilde{d}$ respectively and let D_a and D_d denote the degree of the denominator of $\tilde{a}$ and $\tilde{d}$ respectively.

Suppose first that there exist $r, s \in \mathbf{Z}_{\geq 1}$ with $\gcd(r, s) = 1$ and an $f \in K_\infty$ such that $\tilde{a}^r \tilde{d}^s \frac{\phi(f)}{f}$ is constant. Then we must have $rD_a = sN_d$ and $rN_a = sD_d$, because $\tilde{a}$ and $\tilde{d}$ are reduced.

If $rD_a = sN_d$ and $rN_a = sD_d$ holds then we apply the algorithm for first order q -difference equations to $\tilde{a}^r \tilde{d}^s$ to investigate whether there exist an $f \in K_\infty$ such that $\tilde{a}^r \tilde{d}^s \frac{\phi(f)}{f}$ is constant and reduced. If there exist such an f then we let $T =$

$\begin{pmatrix} f^v & 0 \\ 0 & f^w \end{pmatrix}$, where v, w are chosen such that $vr + ws = 1$. Then $B = \phi(T)\tilde{A}T^{-1}$ is in standard form.

Suppose now that there exists an $r \in \mathbf{Z}_{\geq 1}$ and an $s \in \mathbf{Z}_{\leq -1}$ with $\gcd(r, s) = 1$ and an $f \in K_\infty$ such that $\tilde{a}^r \tilde{d}^s \frac{\phi(f)}{f}$ is constant and reduced. Then we must have $rN_a = -sN_d$ and $rD_a = -sD_d$, because $\tilde{a}$ and $\tilde{d}$ are reduced.

If $rN_a = -sN_d$ and $rD_a = -sD_d$ holds then we apply the algorithm for first order q -difference equations to $\tilde{a}^r \tilde{d}^s$ to investigate whether there exist an $f \in K_\infty$ such that $\tilde{a}^r \tilde{d}^s \frac{\phi(f)}{f}$ is constant and reduced. If there exist such an f then we let $T = \begin{pmatrix} f^v & 0 \\ 0 & f^w \end{pmatrix}$, where v, w are chosen such that $vr + ws = 1$. Then $B = \phi(T)\tilde{A}T^{-1}$ is in standard form.

If none of the two cases above hold then the system $(\tilde{A})$ is already in standard form and the q -difference Galois group is the upper triangular group U .

We will not discuss the completely reducible case because this case is analogous to the reducible but not completely reducible case.

5.4.3 G is imprimitive

If we did not find a solution $u \in K_\infty^*$ for the Riccati equation then the q -difference Galois group G is irreducible. A group G is called imprimitive if $G \subseteq F = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid \alpha\delta \neq 0 \} \cup \{ \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \mid \beta\gamma \neq 0 \}$. In this subsection we determine whether G is imprimitive if we know already that G is irreducible.

Lemma 5.4.6 *Suppose that the q -difference Galois group G of the difference equation $(\#) : \phi^2 y + a\phi y + by = 0$ is irreducible. Then the following statements are equivalent.*

1. G is an imprimitive group.
2. There exists an $r \in K_\infty^*$ such that the equations $(\#)$ and $\phi^2 y + ry = 0$ are equivalent.

Proof. See [Hen96]. $\square$

Suppose now that the equations $(\#) : \phi^2 y + a\phi y + by = 0$ with $a \neq 0$ and $\phi^2 y + ry = 0$ are equivalent. Then there exist $c, d \in K_\infty^*$ such that y is a solution of $(\#)$ if and only if $cy + d\phi y$ is a solution of $\phi^2 y + ry = 0$. In this case $\frac{c}{d}y + \phi y$ satisfies the equation $\phi^2 y + \frac{d}{\phi^2(d)}ry = 0$.

Theorem 5.4.7 *Suppose that the q -difference Galois group G of the equation $(\#) : \phi^2 y + a\phi y + by = 0$, $a \neq 0$ is irreducible. Then G is imprimitive if and only*

if there exists a solution $E \in K_\infty^*$ of the Riccati equation

$$(\#\#) : \quad \phi^2(E)E + (\phi^2(\frac{b}{a}) - \phi(a) + \frac{\phi(b)}{a})E + \frac{\phi(b)b}{a^2} = 0.$$

And if $E \in K_\infty^*$ is a solution of this Riccati equation then y satisfies the equation $(\#)$ if and only if $Dy + \phi y$ satisfies the equation $\phi^2 y + ry = 0$, where $D = E + \frac{b}{a}$ and $r = -a\phi(a) + \phi(b) + a\phi^2(D)$.

Proof. See [Hen96]. $\square$

Remark 5.4.8 We can find the rational solutions of equation $(\#\#)$ by applying the algorithm in subsection 5.4.1 with q replaced by q^2 .

Lemma 5.4.9 The imprimitive subgroups $G \subset Gl(2, \mathbf{C})$ with G/G^0 finite cyclic are

1. $F = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid \alpha\delta \neq 0 \} \cup \{ \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \mid \beta\gamma \neq 0 \}.$
2. $H_n^- = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid (\alpha\delta)^n = 1 \} \cup \{ \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \mid (\beta\gamma)^n = -1 \}$ for $n \in \mathbf{Z}_{\geq 1}.$
3. $H_n^+ = \{ \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \mid (\alpha\delta)^n = 1 \} \cup \{ \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} \mid (\beta\gamma)^n = 1 \}$ for n odd.

Proof. See [Hen96]. $\square$

Consider the system $\phi(\mathbf{y}) = \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} \mathbf{y}$. We can apply the algorithm for first order q -difference equations to cd . Then we will find an $f \in K_\infty^*$ such that $cd\frac{\phi(f)}{f}$ is reduced. Let $T = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}$. Then $B = \phi(T) \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix} T^{-1}$ is in standard form.

5.4.4 G contains $Sl(2, \mathbf{C})$

Consider the system $\phi(\mathbf{y}) = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \mathbf{y}$. If the q -difference Galois group G of this system is neither reducible nor imprimitive, then $G = Gl(2, \mathbf{C})$ or $G = Sl(2, \mathbf{C})_n = \{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid (\alpha\delta - \beta\gamma)^n = 1 \}$. We apply the algorithm for first order q -difference equations to $b = \det \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix}$ and find an $f \in K_\infty^*$ such that $\frac{\phi(f)}{f}b$ is reduced. Let $T = \begin{pmatrix} f & 0 \\ 0 & 1 \end{pmatrix}$. Then $B = \phi(T) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T^{-1}$ is in standard form. This finishes the algorithm.

5.5 Examples

In this section sequences spaces are used in order to make the Picard–Vessiot rings associated to a system of q -difference equations more concrete. The explicit solutions which can be computed are certain sequences which will be called Liouvillian. The second order q -difference equations which will be treated in subsection 5.5.2 are the so-called hypergeometric q -difference equations.

5.5.1 Sequences spaces

Let F be any field. Consider the set of sequences $F^{\mathbf{N}}$. This set forms a ring by using coordinate-wise addition and multiplication. Let J be the ideal of sequences with at most finitely many non-zero terms. Then we define $\mathcal{S}_F = F^{\mathbf{N}}/J$. The map $\rho : \mathcal{S}_F \rightarrow \mathcal{S}_F$ given by $\rho((a_1, a_2, a_3, \dots)) = (a_2, a_3, \dots)$ is well defined on equivalence classes. Moreover, ρ is an automorphism of the ring $\mathcal{S}_F$. For simplicity we will identify an element $\mathbf{a} = (a_1, a_2, a_3, \dots)$ with its equivalence class.

Consider the fields $K_i = \mathbf{C}(z_i)$. We can embed the fields K_i in $\mathcal{S}_{\mathbf{C}}$ by mapping a rational function $f(z_i)$ to the sequence $\mathbf{s}_f = (s_1, s_2, \dots)$, where $s_n = f(q_i^n)$ for all but finitely many $n \in \mathbf{N}$. We will denote the homomorphisms $f \mapsto \mathbf{s}_f$ by ψ . We have $\psi(z_i) = \psi(z_{i+1})^{i+1}$. Hence the embeddings of the fields K_i induce an embedding of the field K_{∞} . It is obvious that $\psi\phi = \rho\psi$. The map $\psi : K_{\infty} \rightarrow \mathcal{S}_{\mathbf{C}}$ is an injective homomorphism because K_{∞} is a field and $\psi(1) = 1$. Therefore from now on we will identify an element $f \in K_{\infty}$ with its image $\mathbf{s}_f$ in $\mathcal{S}_{\mathbf{C}}$.

Theorem 5.5.1 *Consider the system of q -difference equations $(A) : \phi(\mathbf{y}) = A\mathbf{y}$, where $A \in \text{Gl}(n, K_{\infty})$. There exist a q -difference subring $R \subset \mathcal{S}_{\mathbf{C}}$ such that (R, ρ) is a Picard–Vessiot extension associated to the system (A) over the field K_{∞} .*

Proof. For the proof of this theorem we refer to chapter 4 of [PS96]. $\square$

Definition 5.5.2 *We define the ring of Liouvillian sequences $\mathcal{L}$ recursively. $\mathcal{L}$ is the smallest subring of $\mathcal{S}_{\mathbf{C}}$ such that*

1. $K_{\infty} \subset \mathcal{L}$.
2. $\mathbf{a} \in \mathcal{L}$ implies that $\rho(\mathbf{a}) \in \mathcal{L}$
3. $\mathbf{a} \in K_{\infty}$ implies that $\mathbf{b} \in \mathcal{L}$ if $b_{n+1} = a_n b_n$ for all but finitely many $n \in \mathbf{N}_{\geq 1}$.
4. $\mathbf{a} \in \mathcal{L}$ implies that $\mathbf{b} \in \mathcal{L}$ if $b_{n+1} = a_n + b_n$ for all but finitely many $n \in \mathbf{N}_{\geq 1}$.
5. $\mathbf{a} \in \mathcal{L}$ implies that $\mathbf{b} \in \mathcal{L}$ if there exist a $j \in \mathbf{N}_{\geq 1}$ such that $b_{jn} = a_n$ and $b_n = 0$ if $n \not\equiv 0 \pmod j$. In this case we call $\mathbf{b}$ an interlacing of $\mathbf{a}$ with zeroes.

Theorem 5.5.3 Suppose $\mathbf{a} \in \mathcal{S}_{\mathbf{C}}$. Then the following statements are equivalent.

1. $\mathbf{a} \in \mathcal{L}$
2. The sequence $\mathbf{a}$ satisfies a linear q -difference equation over K_{∞} so that the q -difference Galois group G associated to this equation is solvable.

Proof. For the proof we refer to [Hen96]. $\square$

A consequence of the proof of the previous theorem is that all the solutions of a second order q -difference equation $\phi^2 y + a\phi y + by = 0$ are Liouvillian if and only if the difference Galois group G is reducible or irreducible and imprimitive. If the q -difference Galois group G contains $Sl(2, \mathbf{C})$, then there are no Liouvillian solutions of the second order q -difference equation $\phi^2 y + a\phi y + by = 0$.

Example. Let $q = 4$ and $q_2 = 2$. Let $a = 6z$ and $b = 2z^2 - 2z$. Consider the q -difference equation $\phi^2 y + a\phi(y) + by = 0$ and the corresponding Riccati equation $\phi(u)u + au + b = 0$. We are in the case that $v_0(b) \leq 2v_0(a)$ and $v_0(b)$ is odd. Therefore the Riccati equation has not a solution in K_1 . Now we have to apply step 4. of the algorithm to find out whether there are solutions in K_2 . From now on we will consider a and b as elements in $\mathbf{Q}(z_2)$. The Riccati equation reads $\phi(u)u - 6z_2^2 u + 2z_2^4 - 2z_2^2 = 0$. A calculation shows that $S_0 = \{z_2 + O(z_2^2), -z_2 + O(z_2^2)\}$ and $S_{\infty} = \{z_2^2 + O(z_2), \frac{1}{2}z_2^2 + O(z_2)\}$. Further we have $S_p = \{1, z_2, z_2 - 1, z_2 + 1, z_2^2, z_2^2 - z_2, z_2^2 + z_2, z_2^2 - 1, z_2^3 - z_2^2, z_2^3 + z_2^2, z_2^3 - z_2, z_2^4 - z_2^2\}$ and $S_t = \{1\}$. We must have $m = v_0(u) + v_0(p) - v_0(t)$ and $m = v_{\infty}(t) - v_{\infty}(p) - v_{\infty}(u)$. Hence $v_0(p) + v_{\infty}(p) = 1$. Therefore $p = z_2 \pm 1$ and $m = 1$.

Suppose now $u_0 = z_2 + O(z_2^2)$, $u_{\infty} = z_2^2 + O(z_2)$ and $p = z_2 + 1$ then we find $\frac{u_0 t}{cz_2^m p} = \frac{1}{c} + O(z_2)$. Hence $c = 1$. And we find $\frac{u_{\infty} t}{cz_2^m p} = 1 + O(\frac{1}{z_2})$. Now q^e must be equal to 1. Hence $e = 0$. $R = 1$ satisfies the equation $(\ddagger)$ and one finds that $u_1 = z_2 p = z_2^2 + z_2$ is a solution of the Riccati equation in K_2 .

Suppose now $u_0 = -z_2 + O(z_2^2)$, $u_{\infty} = z_2^2 + O(z_2)$ and $p = z_2 - 1$ then we find $\frac{u_0 t}{cz_2^m p} = \frac{1}{c} + O(z_2)$. Hence $c = 1$. And we find $\frac{u_{\infty} t}{cz_2^m p} = 1 + O(\frac{1}{z_2})$. Now q^e must be equal to 1. Hence $e = 0$. $R = 1$ satisfies the equation $(\ddagger)$ and one finds that $u_2 = z_2 p = z_2^2 - z_2$ is a solution of the Riccati equation in K_2 .

A calculation shows that the other combinations of u_0 , u_{∞} and p do not yield any solution of the Riccati equation in K_2 . The difference equation $\phi^2 y + a\phi y + by = 0$ is equivalent with the system $\phi \mathbf{y} = \begin{pmatrix} u_1 & 0 \\ 0 & u_2 \end{pmatrix} \mathbf{y}$. This system is already

in standard form. Hence $G = \{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a \in \mathbf{C}^*, d \in \mathbf{C}^* \}$.

Two linearly independent elementary solutions of the q -difference equation in the ring $\mathcal{S}_{\mathbf{C}}$ are $\mathbf{c}$ and $\mathbf{d}$, where $c_n = \prod_{k=1}^{n-1} (2^{2k} + 2^k)$ and $d_n = \prod_{k=1}^{n-1} (2^{2k} - 2^k)$. The

sequence $\mathbf{c} \in \mathcal{S}_{\mathbf{C}}$ satisfies the first order q -difference equation $\phi(y) = u_1 y$ and the sequence $\mathbf{d} \in \mathcal{S}_{\mathbf{C}}$ satisfies the first order q -difference equation $\phi(y) = u_2 y$.

5.5.2 Hypergeometric q -difference equations

In this section we apply the algorithm to some cases of the hypergeometric q -difference equation which is given by

$$\phi^2(y) + \frac{(-4 + q^\alpha + q^\beta)z + 3 - q^{\gamma-1}}{z-1}\phi(y) + \frac{(2 - q^\alpha)(2 - q^\beta)z - 2 + q^{\gamma-1}}{z-1}y = 0.$$

As usual we will identify this equation with the system (A) : $\phi \mathbf{y} = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \mathbf{y}$, where $a = \frac{(-4+q^\alpha+q^\beta)z+3-q^{\gamma-1}}{z-1}$ and $b = \frac{(2-q^\alpha)(2-q^\beta)z-2+q^{\gamma-1}}{z-1}$.

Case 1. We will analyse the case where α, β and γ are rational parameters and q is transcendental. Note that the hypergeometric equation is symmetric in the parameters α and β . This restricts the number of possibilities we have to consider.

Theorem 5.5.4 *Let G denote the q -difference Galois group of the hypergeometric q -difference equation.*

1. If $\alpha = 0, \beta = 0$ and $\gamma = 1$ then $G = \{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbf{C} \}$.
2. If $(\alpha = 0 \text{ and } \beta = \gamma - 1)$ or $(\alpha = \gamma - 1 \text{ and } \beta = 0)$ and $\gamma \neq 1$ then $G = \{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \mid d \in \mathbf{C}^* \}$.
3. If $(\alpha = 0 \text{ and } \beta \neq \gamma - 1)$ or $(\alpha \neq \gamma - 1 \text{ and } \beta = 0)$ then $G = \{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \mid b \in \mathbf{C}, d \in \mathbf{C}^* \}$.
4. If $(\alpha \neq 0 \text{ and } \beta = \gamma - 1)$ or $(\alpha = \gamma - 1 \text{ and } \beta \neq 0)$ then $G = \{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid b \in \mathbf{C}, a, d \in \mathbf{C}^* \}$.
5. If $\alpha \neq 0, \alpha \neq \gamma - 1, \beta \neq 0$ and $\beta \neq \gamma - 1$ then $G = Gl(2, \mathbf{C})$.

Proof. Consider the rather special cases that $(\alpha = 0 \text{ and } \beta = \gamma - 1)$ or $(\alpha = \gamma - 1 \text{ and } \beta = 0)$. In these cases the hypergeometric q -difference equation simplifies to the equation $\phi^2(y) - (3 - q^{\gamma-1})\phi(y) + (2 - q^{\gamma-1})y = 0$.

If moreover $\gamma = 1$, then we get the equation $\phi^2(y) - 2\phi(y) + y = 0$. In this case $u = 1$ is the only solution of the corresponding Riccati equation. Hence the q -difference Galois group is reducible but not completely reducible. Let $T =$

$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ and $B = \phi(T)AT^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Obviously the equivalent system $(B) : \phi(\mathbf{y}) = B\mathbf{y}$ is in standard form. Hence the q -difference Galois group G is equal to the group $\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbf{C} \}$.

Suppose now that $\gamma \neq 0$. Clearly $u = 1$ and $u = 2 - q^{\gamma-1}$ are the only solutions of the corresponding Riccati equation. Hence the q -difference Galois group G is completely irreducible if $\gamma \neq 0$. In that case the q -difference equation is equivalent to the system of difference equations $\phi\mathbf{y} = \begin{pmatrix} 1 & 0 \\ 0 & 2 - q^{\gamma-1} \end{pmatrix}\mathbf{y}$. This system is in standard form. The q -difference Galois group G is equal to the group $\{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \mid d \in \mathbf{C}^* \}$, because q is transcendental and γ is rational.

From now on we will exclude the cases that $(\alpha = 0$ and $\beta = \gamma - 1)$ or $(\alpha = \gamma - 1$ and $\beta = 0)$.

Consider the Riccati equation $(\dagger) : \phi(u)u + au + b = 0$. A simple calculation shows that $S_0 = \{1 + O(z), 2 - q^{\gamma-1} + O(z)\}$ and $S_\infty = \{2 - q^\alpha + O(\frac{1}{z}), 2 - q^\beta + O(\frac{1}{z})\}$. Further we have $S_p = \{1, z - \frac{2 - q^{\gamma-1}}{(2 - q^\alpha)(2 - q^\beta)}\}$ and $S_t = \{1, z - q\}$. For all choices $u_0 \in S_0, p \in S_p$ and $t \in S_t$ we find $m = 0$. For all $u_\infty \in S_\infty$ we have $v_\infty(u_\infty) = 0$. Hence we must have $\deg_z(p) = \deg_z(t)$. Now we have to consider four different possibilities.

The first combination is $u_0 = 1 + O(z), p = 1, t = 1$ and $u_\infty = 2 - q^\alpha + O(\frac{1}{z})$. We must have $\frac{u_0 t}{cp} = 1 + O(z)$. Hence $c = 1$. And we compute $\frac{u_\infty t}{cp} = 2 - q^\alpha + O(\frac{1}{z})$. So $d = 2 - q^\alpha$. We have d is of the form q^e with $e \in \mathbf{Z}_{\geq 0}$ if and only if $\alpha = 0$. In that case $e = 0$ and $R = 1$ turns out to be a solution of the equation $(\ddagger)$. Therefore $u = c \frac{\phi(R)p}{Rt} = 1$ is a solution of the Riccati equation if $\alpha = 0$.

The second combination is $u_0 = 2 - q^{\gamma-1} + O(z), p = 1, t = 1$ and $u_\infty = 2 - q^\alpha + O(\frac{1}{z})$. We must have $\frac{u_0 t}{cp} = 1 + O(z)$. Hence $c = 2 - q^{\gamma-1}$. And we compute $\frac{u_\infty t}{cp} = \frac{2 - q^\alpha}{2 - q^{\gamma-1}} + O(\frac{1}{z})$. So $d = \frac{2 - q^\alpha}{2 - q^{\gamma-1}}$. We have d is of the form q^e with $e \in \mathbf{Z}_{\geq 0}$ if and only if $\alpha = \gamma - 1$. In that case $e = 0$ and $R = 1$ turns out to be a solution of the equation $(\ddagger)$. Therefore $u = c \frac{\phi(R)p}{Rt} = 2 - q^{\gamma-1}$ is a solution of the Riccati equation if $\alpha = \gamma - 1$.

The third combination is $u_0 = 1 + O(z), p = z - \frac{2 - q^{\gamma-1}}{(2 - q^\alpha)(2 - q^\beta)}, t = z - q$ and $u_\infty = 2 - q^\alpha + O(\frac{1}{z})$. We must have $\frac{u_0 t}{cp} = 1 + O(z)$. Hence $c = \frac{2 - q^{\gamma-1}}{q(2 - q^\alpha)(2 - q^\beta)}$. And we compute $\frac{u_\infty t}{cp} = \frac{q(2 - q^\alpha)^2(2 - q^\beta)}{2 - q^{\gamma-1}} + O(\frac{1}{z})$. So $d = \frac{q(2 - q^\alpha)^2(2 - q^\beta)}{2 - q^{\gamma-1}}$. Now d is not of the form q^e with $e \in \mathbf{Z}_{\geq 0}$, unless we have $\alpha = 0$ and $\beta = \gamma - 1$. But we have excluded this situation. Hence this combination does not yield a rational solution of the Riccati equation.

The fourth combination is $u_0 = 2 - q^{\gamma-1} + O(z), p = z - \frac{2 - q^{\gamma-1}}{(2 - q^\alpha)(2 - q^\beta)}, t = z - q$ and $u_\infty = 2 - q^\alpha + O(\frac{1}{z})$. We must have $\frac{u_0 t}{cp} = 1 + O(z)$. Hence $c = \frac{1}{q(2 - q^\alpha)(2 - q^\beta)}$. And we compute $\frac{u_\infty t}{cp} = q(2 - q^\alpha)^2(2 - q^\beta) + O(\frac{1}{z})$. So $d = q(2 - q^\alpha)^2(2 - q^\beta)$.

Now d is of the form q^e with $e \in \mathbf{Z}_{\geq 0}$ if and only if $\alpha = \beta = 0$. Then $e = 1$. We substitute $R = z + r$ in $(\dagger)$. (See subsection 5.4.1). We get the equation $\frac{1}{q^2}(q^2z+r)\phi(p)p(z-1) + \frac{1}{q}(qz+r)\phi(t)p(-2z+3-q^{\gamma-1}) + (z+r)\phi(t)t(z-(2-q^{\gamma-1})) = 0$. After simplifying this equation we get two linear equations for r that contradict each other. Hence this combination does not yield any solution of the Riccati equation.

We found that there is exactly one solution of the Riccati equation in K if $\alpha = 0$ and $\beta \neq \gamma - 1$ or $\alpha = \gamma - 1$ and $\beta \neq 0$ or $\beta = 0$ and $\alpha \neq \gamma - 1$ or $\beta = \gamma - 1$ and $\alpha \neq 0$. Applying step 4 of the algorithm for solving the Riccati equation we find that all the solutions of the Riccati equation in K_∞ are already in K . This computation is similar to the computations above.

Suppose that $\alpha = 0$ and $\beta \neq \gamma - 1$. Let $T = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$. Then we get $B = \phi(T)AT^{-1} = \begin{pmatrix} 1 & \frac{(2-q^\beta)z-(2-q^{\gamma-1})}{z-1} \\ 0 & \frac{(2-q^\beta)z-(2-q^{\gamma-1})}{z-1} \end{pmatrix}$. System (B) is equivalent to system (A) . Moreover system (B) is in standard form because q is transcendental and $\beta \neq \gamma - 1$. The differential Galois group $G = \{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \mid b \in \mathbf{C}, d \in \mathbf{C}^* \}$.

Suppose that $\alpha = \gamma - 1$ and $\beta \neq 0$. Let $T = \begin{pmatrix} -1 + 2^{\gamma-1} & 1 \\ -2 + 2^{\gamma-1} & 1 \end{pmatrix}$. Then we get $B = \phi(T)AT^{-1} = \begin{pmatrix} 2 - q^{\gamma-1} & \frac{(1+q^{\gamma-1}-q^\beta)z-q^{\gamma-1}}{(2-q^\beta)z-1} \\ 0 & \frac{(2-q^\beta)z-1}{z-1} \end{pmatrix}$. System (B) is equivalent to system (A) . Moreover system (B) is in standard form because q is transcendental and $\beta \neq 0$. The q -difference Galois group $G = \{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid b \in \mathbf{C}, a, d \in \mathbf{C}^* \}$.

If $\alpha \neq 0$, $\alpha \neq \gamma - 1$, $\beta \neq 0$ and $\beta \neq \gamma - 1$ then the q -difference Galois group is irreducible. By using the algorithms of section 5.4.3 and 5.4.4 one can show that in this case the q -difference Galois group G is the group $Gl(2, \mathbf{C})$. $\square$

It is possible to give two linearly independent Liouvillian solution for the hypergeometric q -difference equations in all those cases where the q -difference Galois group G is not the group $Gl(2, \mathbf{C})$.

Case 2. If q is not transcendental then the situation can be different. For instance let $\alpha = \beta = \gamma = 1$. Then the equation simplifies to $\phi^2(y) + \frac{(-4+2q)z+2}{z-1}\phi(y) + \frac{(2-q)^2z-1}{z-1}y = 0$. If q is transcendental then the q -difference Galois group G is the group $Gl(2, \mathbf{C})$. But if $q = -\frac{1}{2} \pm \frac{1}{2}\sqrt{-7}$, that is q is a root of the polynomial $x^2 + x + 2$, then the difference Galois group G turns out to be reducible. From now on we will assume that $q = -\frac{1}{2} \pm \frac{1}{2}\sqrt{-7}$.

Consider the corresponding Riccati equation $(\dagger) : \phi(u)u + au + b = 0$, where $a = \frac{(-4+2q)z+2}{z-1}$ and $b = \frac{(2-q)^2z-1}{z-1}$. We find $S_0 = \{1 + O(z)\}$ and $S_\infty = \{2 - q +$

$O(\frac{1}{z})\}$. Further we have $S_p = \{1, z - \frac{1}{(2-q)^2}\}$ and $S_t = \{1, z - q\}$. We must have $\deg_z(p) = \deg_z(t)$. Hence we have to consider two combinations.

The first combination is $u_0 = 1 + O(z)$, $p = 1$, $t = 1$, and $u_\infty = 2 - q + O(\frac{1}{z})$. We must have $\frac{u_0 t}{cp} = 1 + O(z)$. Hence $c = 1$. We compute $\frac{u_\infty t}{cp} = 2 - q + O(\frac{1}{z})$. So $d = 2 - q$. We have $2 - q = q^3$. Hence $e = 3$. We substitute $R = z^3 + r_2 z^2 + r_1 z + r_0$ in the equation $(\ddagger)$. And we find the solution $R = z^3 - \frac{3q+1}{16} z^2 + \frac{5q+7}{64} z + \frac{5q+7}{64} = (z - \frac{1-q}{4})(z^2 + \frac{3-7q}{16} z - \frac{1-3q}{16})$. Now $u = \frac{\phi(R)}{R}$ is a solution of the Riccati equation.

The second combination is $u_0 = 1 + O(z)$, $p = z - \frac{1}{(2-q)^2}$, $t = z - q$, and $u_\infty = 2 - q + O(\frac{1}{z})$. We must have $\frac{u_0 t}{cp} = 1 + O(z)$. Hence $c = \frac{1}{q(2-q)^2}$. We compute $\frac{u_\infty t}{cp} = q(2-q)^3 + O(\frac{1}{z})$. So $d = q(2-q)^3 = q^{10}$. Hence $e = 10$. We substitute $R = z^{10} + r_9 z^9 + \dots + r_1 z + r_0$ in $(\ddagger)$. After simplifying we get eleven linear equations for the ten variables r_i . There are no solutions. We conclude that the second combination does not yield any solution of the Riccati equation.

We have $u = \frac{\phi(R)}{R}$ with $R = (z - \frac{1-q}{4})(z^2 + \frac{3-7q}{16} z - \frac{1-3q}{16})$ is the only solution of the Riccati equation in K_∞ . Let $T = \begin{pmatrix} 1-u & 1 \\ -u & 1 \end{pmatrix}$. Then we get

$B = \phi(T) \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} T^{-1} = \begin{pmatrix} u & 1-u+b/u \\ 0 & b/u \end{pmatrix}$. System (B) is not yet in standard form. Note that $u = \frac{\phi(R)}{R}$ and $b = \frac{\phi(s)}{s}$, where $s = (q^5 z - 1)(q^4 z - 1) \dots (qz - 1)(z - 1)$. Let $S = \begin{pmatrix} \frac{1}{R} & 0 \\ 0 & \frac{R}{s} \end{pmatrix}$. Then we get $C = \phi(S) B S^{-1} = \begin{pmatrix} 1 & f \\ 0 & 1 \end{pmatrix}$, where $f = \frac{(u-u^2+b)s}{\phi(R)^2}$. System (C) is in standard form. Therefore the q -difference Galois group G is equal to the group $\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbf{C} \}$.

Chapter 6

On the classification of a class of q -difference equations

6.1 Introduction

Let q be an m th root of unity. The aim of this article is to classify the q -difference equations over the field $K = \mathbf{C}(z)$. The classification is rather similar to the classification of differential and difference equations in characteristic p . See [Put95] and [PS96]. Further some Picard–Vessiot theory will be developed for these equations.

6.2 Picard–Vessiot Theory

Let $\phi : \mathbf{C}(z) \rightarrow \mathbf{C}(z)$ be an $\mathbf{C}$ –linear automorphism given by $\phi(z) = qz$, where q is an m th root of unity. Consider the system of difference equation $(A) : \phi \mathbf{y} = A\mathbf{y}$, where $A \in Gl(n, \mathbf{C}(z))$. (We restrict ourselves to equations with $A \in Gl(n, \mathbf{C}(z))$ in order to guarantee that we get n independent solutions.

Definition 6.2.1 *A ring R together with an automorphism $\phi_R : R \rightarrow R$ is called a Picard–Vessiot extension over $\mathbf{C}(z)$ associated with system (A) if*

1. *R is a commutative ring, $R \subseteq \mathbf{C}(z)$ and $\phi_R|_{\mathbf{C}(z)} = \phi$.*
2. *The only ϕ_R –invariant ideals of R are 0 and R*
3. *There exists a matrix $U \in Gl(n, R)$ such that $\phi_R(U) = AU$. (Such a matrix U is called a fundamental matrix for the system (A) .)*
4. *R is minimal with respect to the conditions 1, 2 and 3 or equivalently if $U = (u_{ij}) \in Gl(n, R)$ is a fundamental matrix for the matrix for the system (A) then $R = \mathbf{C}(z)[u_{11}, \dots, u_{nn}, \frac{1}{\det(U)}]$.*

From now on we will denote ϕ_R also by ϕ . For a given system of q -difference equations $(A) : \phi \mathbf{y} = A \mathbf{y}$ one can construct a Picard–Vessiot extension in the following way. Let (x_{ij}) denote a matrix of indeterminates and let $\det$ denote the determinant of this matrix. On the $\mathbf{C}(z)$ -algebra $\mathbf{C}(z)[x_{ij}, \frac{1}{\det}]$ one extends the automorphism ϕ by setting $\phi(x_{ij}) = A(x_{ij})$. Let I be an ideal of $\mathbf{C}(z)[x_{ij}, \frac{1}{\det}]$, which is maximal among the proper ϕ -invariant ideals. Then $\mathbf{C}(z)[x_{ij}, \frac{1}{\det}]/I$ is a Picard–Vessiot ring for the system of equations (A) . Any Picard–Vessiot ring is of this form.

Unlike the case, where q is not a root of unity, there is no uniqueness of Picard–Vessiot rings, due to the fact that in our case the field of constants $\mathbf{C}(z^m) \subset \mathbf{C}(z)$ is not algebraically closed. For instance assume that $q = 1$ and consider the first order equation $\phi(y) = -y$. Then $R_c := \mathbf{C}(z)[u, u^{-1}]/(u^2 - c)$ is a Picard–Vessiot ring for all $c \in \mathbf{C}(z)^*$, because if $c \in \mathbf{C}(z)^*$ is a square then the only nontrivial ideals are generated by the cosets of $u - \sqrt{c}$ and $u + \sqrt{c}$ and these ideals are not ϕ -invariant. We have $R_{c_1} \cong R_{c_2}$ if and only if $\frac{c_1}{c_2} \in \mathbf{C}(z)^*$ is a square and this is not always the case.

If q is not a root of unity, then there is a unique (unique up to $\mathbf{C}$ -linear isomorphisms commuting with ϕ) Picard–Vessiot extension associated to every system of q -difference equations. See [PS96]. Then the q -difference Galois group of an equation is the group of $\mathbf{C}$ -linear automorphisms of the Picard–Vessiot ring commuting with ϕ . Unfortunately in our case there is not a unique Picard–Vessiot ring for every system of q -difference equations. Hence it is not possible to define a q -difference Galois group of an equation in this way. However in section 4 we will use the theory of Tannakian categories for a suitable definition of the q -difference Galois group. The idea is to compare q -difference modules over $\mathbf{C}(z)$ with modules over the ring $Z = L[t, t^{-1}]$, where L is the field of constants $\mathbf{C}(z^m)$, because modules over $Z = L[t, t^{-1}]$ are easier to understand.

To a system of q -difference equations one can associate a q -difference module. If a difference equation $\phi \mathbf{y} = A \mathbf{y}$ with $A \in Gl(n, \mathbf{C}(z))$ is given then one defines a q -difference module structure on $\mathbf{C}(z)^n$ by setting $\Phi \mathbf{y} = A^{-1} \phi \mathbf{y}$. We have $\Phi a \mathbf{y} = \phi(a) \Phi \mathbf{y}$ if $a \in \mathbf{C}(z)$. In the next section we will classify the q -difference modules over the field $\mathbf{C}(z)$ if q is a root of unity.

6.3 Classification of q -Difference Modules

Let q be an m th root of unity and let $\mathcal{D}$ be the skew Laurent polynomial ring $\mathbf{C}(z)[\Phi, \Phi^{-1}]$, where the multiplication is fixed by the rule $\Phi z = qz\Phi$. In this section we will classify the left $\mathcal{D}$ -modules which have finite dimension over $\mathbf{C}(z)$.

Lemma 6.3.1 *Let Z be the center of $\mathcal{D}$. Then*

1. $Z = \mathbf{C}(z^m)[\Phi^m, \Phi^{-m}]$ is a commutative Laurent polynomial ring.
2. $\mathcal{D}$ is a free Z -module of rank m^2 .

3. Let $\text{Quot}(Z)$ denote the field of quotients of Z . Then $\text{Quot}(Z) \otimes_Z \mathcal{D}$ is a skew field with center $\text{Quot}(Z)$ and dimension m^2 over its center.

Proof.

1. For all integers $j \in \mathbf{Z}$ one has $\Phi^j z = q^j z \Phi^j$. This implies that $\Phi^j \in Z$ if and only if j is a multiple of m . Further one has $\Phi z^j = q^j z^j \Phi$. Hence $z^j \in Z$ if and only if j is a multiple of m . So we have $Z \supseteq \mathbf{C}(z^m)[\Phi^m, \Phi^{-m}]$. Any $f \in \mathcal{D}$ can be written uniquely as $f = \sum_{0 \leq i, j < m} f_{ij} z^i \Phi^j$ with all $f_{ij} \in \mathbf{C}(z^m)[\Phi^m, \Phi^{-m}]$. Suppose that $f \in Z$. Then $0 = zf - fz = \sum_{0 \leq i, j < m} (1 - q^j) f_{ij} z^{i+1} \Phi^j$. Hence if $j \neq 0$ then $f_{ij} = 0$ and so $f = \sum_{0 \leq i < m} f_{i,0} z^i$. And $0 = \Phi f - f \Phi = \sum_{0 \leq i < m} (q^i - 1) f_{i,0} z^i \Phi$ implies $f = f_{0,0} \in \mathbf{C}(z^m)[\Phi^m, \Phi^{-m}]$. We conclude that $Z = \mathbf{C}(z^m)[\Phi^m, \Phi^{-m}]$.
2. This is already shown in part 1 of the proof.
3. If $f \in \mathcal{D}$ then one can write $f = \sum_{i \in \mathbf{Z}} f_i \Phi^i$ with all $f_i \in \mathbf{C}(z)$. We define the discrete valuation v by $v(f) = \max\{k \mid f_k \neq 0\}$ and $v(0) = -\infty$. We have $v(fg) = v(f) + v(g)$. Hence $\mathcal{D}$ and $\text{Quot}(Z) \otimes_Z \mathcal{D}$ have no zero divisors and $\text{Quot}(Z) \otimes_Z \mathcal{D}$ must be a skew field with center $\text{Quot}(Z)$ and dimension m^2 over its center. $\square$

Lemma 6.3.2 Let $\mathfrak{m}$ denote a maximal ideal of Z with residue field $L = Z/\mathfrak{m}$. Then $\mathcal{D}/\mathfrak{m}\mathcal{D} = L \otimes_Z \mathcal{D}$ is isomorphic to the matrix ring $M(m \times m, L)$.

Proof. First we will proof that $L \otimes_Z \mathcal{D}$ is a central simple algebra over L with dimension m^2 over its center. Let $I \neq 0$ be a two-sided ideal of $L \otimes_Z \mathcal{D}$. We must show that I is the unit ideal. Suppose $f \in I$ and $f \neq 0$. Then f can be written uniquely in the form $f = \sum_{0 \leq i, j < m} f_{ij} z^i \Phi^j$, where $f_{ij} \in L$ for all i, j . Let $f_1 = f - qz^{-1}fz \in I$. Then $f_1 = \sum_{0 \leq j < m-1} f_{ij}(1 - q^{1+j})$. Note that the $m-1$ th coefficient of f_1 with respect to Φ is 0. We define recursively $f_i = f_{i-1} - q^i z^{-1} f_{i-1} z$. We have $f_i \in I$ for all i . Let $g_0 = f_{m-1}$. Then we can write $g_0 = \sum_{0 \leq i < m} a_i z^i$, where $a_i \in L$ for all i . We define recursively $g_i = g_{i-1} - q^i \Phi g_{i-1} \Phi^{-1}$. We have $g_i \in I$ for all i and $g_{m-1} \in L$. Hence I is the unit ideal. As in Lemma 6.3.1 one can easily verify that L is the center of $L \otimes_Z \mathcal{D}$. The dimension of $L \otimes_Z \mathcal{D}$ over L is m^2 . The classification of central simple algebras tells us that $L \otimes_Z \mathcal{D}$ is isomorphic to a matrix algebra $M(d \times d, S)$ over a skew field S containing L with $[S : L] = e^2$ where $n = ed$. But L is a C_1 -field of characteristic 0. This implies that there does not exist such skew field extensions, that is $e = 1$. See [Gre69]. Hence $L \otimes_Z \mathcal{D}$ is isomorphic to the matrix ring $M(m \times m, L)$. $\square$

Theorem 6.3.3 (*Classification of irreducible $\mathcal{D}$ -modules*) *There is a bijective correspondence between the irreducible left $\mathcal{D}$ -modules of finite dimension over $K = \mathbf{C}(z)$ and the maximal ideals of Z .*

Proof. Suppose M is an irreducible left $\mathcal{D}$ -module which has finite dimension over the field K . Then the set $\{f \in Z \mid fM = 0\}$ is a non trivial ideal generated by some polynomial F . Suppose that F has a non-trivial factorization $F = F_1 F_2$. The submodule $F_1 M$ is nonzero and must then be equal to M . Now $F_2 M = F_2 F_1 M = 0$ contradicts the definition of F . It follows that F is an irreducible polynomial. Let $\mathfrak{m}$ be the ideal generated by F and let L denotes its residue field. We can consider M as an irreducible $L \otimes_Z \mathcal{D}$ -module and then M must be isomorphic to a vectorspace of dimension m with the natural action of the matrix algebra $M(m \times m, L)$ on it. $\square$

Lemma 6.3.4 *Let F be an irreducible element of Z and let $\mathfrak{m}$ denote the maximal ideal generated by F . Further let $\hat{Z}_F$ denote the completion of the localisation $Z_{\mathfrak{m}}$. That is $\hat{Z}_F$ is the projective limit of the rings $Z/\mathfrak{m}^n$. Then the algebra $\hat{Z}_F \otimes_Z \mathcal{D}$ is isomorphic to $M(m \times m, \hat{Z}_F)$.*

Proof. We will denote the image of Φ^m in $Z/\mathfrak{m}^n$ by t_n . By induction we will construct a sequence of elements $c_n \in Z/\mathfrak{m}^n[z]$ such that $\prod_{i=0}^{m-1} c_n(q^i z) = t_n$ and $c_{n+1} \equiv c_n$ modulo F^n for all $n \geq 1$.

The norm map $N : L[z] \rightarrow L$ given by $c \mapsto \prod_{i=0}^{m-1} c(q^i z)$ is surjective because $L[z]$ is a finite cyclic field extension of L and L is a C_1 -field being a finite field extension of the field $\mathbf{C}(z^m)$. Hence there exists an element $c_1 \in Z/\mathfrak{m}$ such that $N(c_1) = t_1$. Note that $c_1 \neq 0$ because $t_1 \neq 0$.

Let $c_n \in Z/\mathfrak{m}^n$ be constructed. Take some $d \in Z/\mathfrak{m}^{n+1}[z]$ with image c_n and put $c_{n+1} = d + F^n f \in Z/\mathfrak{m}^{n+1}[z]$. Then $\prod_{i=0}^{m-1} c_{n+1}(q^i z) = \prod_{i=0}^{m-1} d(q^i z) + F^n \sum_{i=0}^{m-1} f(q^i z) \prod_{j \neq i} d(q^j z)$. Because the image of t_{n+1} in $Z/\mathfrak{m}^n$ is equal to t_n we have $t_{n+1} - \prod_{i=0}^{m-1} d(q^i z) = gF^n$ in for a certain $g \in Z/\mathfrak{m}^{n+1}$. Let $\tilde{g}$ be the image of g in L .

Then we want to find an element $\tilde{f} \in L[z]$ such that $\sum_{i=0}^{m-1} \tilde{f}(q^i z) \prod_{j \neq i} c_1(q^j z) = \tilde{g}(z)$. That is always possible. One can take $\tilde{f} = \frac{\tilde{g}}{\sum_{i=1}^{m-1} c_1(q^i z)}$. Let $f \in Z/\mathfrak{m}^{n+1}[z]$ be

an element such that the image of f in $L[z]$ is equal to $\tilde{f}$. Then $c_{m+1} = d + F^n f$ satisfies $\prod_{i=0}^{m-1} c_{n+1}(q^i z) = t_{n+1}$.

Let $t_{\infty} \in \hat{Z}_F$ be the projective limit of the t_n and let $c_{\infty} \in \hat{Z}_F[z]$ be the projective limit of the c_n . Then c_{∞} satisfies also $\prod_{i=0}^{m-1} c_{\infty}(q^i z) = t_{\infty}$. On the free

module $\hat{Z}_F[z]e$ over $\hat{Z}_F[z]$ of rank 1 one defines the operator Φ by $\Phi e = c_\infty e$. The equality $\prod_{i=0}^{m-1} c_\infty(q^i z) = t_\infty$ implies that $\hat{Z}_F[z]e$ is a left $\hat{Z}_F \otimes_Z \mathcal{D}$ -module. The natural map

$$\hat{Z}_F \otimes_Z \mathcal{D} \rightarrow \text{End}_{\hat{Z}_F}(\hat{Z}_F[z]e) \cong M(m \times m, \hat{Z}_F)$$

is a homomorphism of $\hat{Z}_F$ -algebras. It is an isomorphism because it is an isomorphism modulo the ideal $\mathfrak{m} = (F)$. $\square$

Theorem 6.3.5 (*Classification of indecomposable $\mathcal{D}$ -modules*) *There is a bijective correspondence between indecomposable left $\mathcal{D}$ -modules of finite dimension over $K = \mathbf{C}(z)$ and the set of powers of the maximal ideals of Z .*

Proof. Let M be an indecomposable left $\mathcal{D}$ -module of finite dimension over K . The set $\{f \in Z \mid fM = 0\}$ is a non-trivial ideal in Z generated by some polynomial F . If F factors as $F_1 F_2$ with coprime F_1 and F_2 then one can write $1 = F_1 G_1 + F_2 G_2$ and any $m \in M$ can be written as $F_1 G_1 m + F_2 G_2 m$. Further $F_1 M \cap F_2 M = \{0\}$, because $m \in F_1 M \cap F_2 M$ implies that $m = (F_1 G_1 + F_2 G_2)m = 0$. Hence $M = F_1 M \oplus F_2 M$. This contradicts the assumption that M is indecomposable. Hence the annihilator of an indecomposable module must have the form (F^m) , where (F) is a monic and irreducible element in Z . Therefore any indecomposable left $\mathcal{D}$ -module can be identified with an indecomposable finitely generated module over $\hat{Z}_F \otimes \mathcal{D} \cong M(m \times m, \hat{Z}_F)$ (lemma 6.3.4), annihilated by some power of a monic irreducible polynomial $F \in Z$.

Morita's theorem gives an equivalence between $\hat{Z}_F$ -modules and $M(m \times m, \hat{Z}_F)$ -modules. (See [Ren75], theorem 1.3.16 and proposition 1.3.17.) In particular, every finitely generated indecomposable module has the form $I(F^n) := (\hat{Z}_F[z]e)/(F^n) \cong Z/(F^n)[z]e_n$. The structure as left $\mathcal{D}$ -module is given by $\Phi(e) = c_\infty e$ and $\Phi(e_n) = c_n e_n$, where $c_n \in Z/(F^n)[z]$ is the image of c_∞ . (See the proof of lemma 6.3.4.) $\square$

Theorem 6.3.6 *Every left $\mathcal{D}$ -module of finite dimension over K is a finite direct sum $\bigoplus_{F,m} I(F^m)^{e(F,m)}$, where F runs through a set of generators of the different maximal ideals of Z and $m \geq 0$. The numbers $e(F, m)$ are uniquely determined by M .*

Proof. The first statement is an immediate consequence of theorem 6.3.5. The numbers $e(F, m)$ are uniquely determined by M since they can be computed in terms of the dimension over K of the kernels of multiplication with F^i on M . $\square$

We have seen that there is a bijective correspondence between left $\mathcal{D}$ -modules of finite dimension over $K = \mathbf{C}(z)$ and Z -modules of finite dimension over $\mathbf{C}(z^m)$. We can make this correspondence more precise. But first we want to define tensor products. The tensor product for $\mathcal{D}$ -modules M and N over $K = \mathbf{C}(z)$ is the

tensor product $M \otimes_K N$ with the operation of Φ given by $\Phi(m \otimes n) = \Phi(m) \otimes \Phi(n)$. Let L be any field and let $FMod_{L[t, t^{-1}]}$ denote the category of the modules over $L[t, t^{-1}]$, which have finite dimension over L . For this abelian category we define the tensor product of two monomials M and N as $M \otimes_L N$ with the operation of t given by $t(m \otimes n) = (tm) \otimes (tn)$. This describes the tensor product for the category of Z -modules of finite dimension over $\mathbf{C}(z^m)$.

Theorem 6.3.7 (*An equivalence of categories*) *There exists an equivalence $\mathcal{F}$ of the category of Z -modules of finite dimension over $\mathbf{C}(z^m)$ onto the category of left $\mathcal{D}$ -modules of finite dimension over $K = \mathbf{C}(z)$. Moreover $\mathcal{F}$ is exact, $\mathbf{C}(z^m)$ -linear and preserves tensor products.*

Proof. First we define the functor $\mathcal{F}$. Let $\hat{Z}$ denote the completion of Z with respect to the set of all nonzero ideals. Then $\hat{Z} = \prod_F \hat{Z}_F$, where the product is taken over a set of polynomials generating the different maximal ideals of Z . The modules over Z of finite dimension over $\mathbf{C}(z^m)$ coincide with the $\hat{Z}$ -modules of finite dimension over $\mathbf{C}(z^m)$. Let $\hat{\mathcal{D}} = \hat{Z} \otimes \mathcal{D}$. The left $\mathcal{D}$ -modules of finite dimension over K coincide with the left $\hat{\mathcal{D}}$ -modules of finite dimension over K . Consider an irreducible polynomial $F \in Z$. By lemma 6.3.4 there exists a left $\hat{\mathcal{D}}$ -module $\hat{Z}_F[z]e_\infty$ with the action of Φ given by $\Phi e_\infty = c_\infty e_\infty$. We will denote this module by $\mathcal{Q}_F$. Let the left $\hat{\mathcal{D}}$ -module $\mathcal{Q}$ be the product of all the $\mathcal{Q}_F$ where F runs through a set of generators of all the different maximal ideals of Z . Then $\mathcal{Q} = \hat{Z}[z]e$ and the action of Φ on $\mathcal{Q}$ is given by $\Phi e = ce$ with a $c \in \hat{Z}[z]$ satisfying $\prod_{i=0}^{m-1} c(q^i z) = t$, where $t \in \hat{Z}$ denotes the image of Φ^m .

For every Z -module M of finite dimension over $\mathbf{C}(z^m)$ one regards M as a $\hat{Z}$ -module and one defines a left $\hat{\mathcal{D}}$ -module $\mathcal{F}(M) := M \otimes_{\hat{Z}} \mathcal{Q}$. This $\hat{\mathcal{D}}$ -module has finite dimension and can also be considered as a left $\mathcal{D}$ -module of finite dimension. For morphisms $\phi : M \rightarrow N$ of Z -modules of finite dimension we define $\mathcal{F}(\phi) := \phi \otimes 1 : \mathcal{F}(M) \rightarrow \mathcal{F}(N)$. It is clear that $\mathcal{F}$ is a $\mathbf{C}(z^m)$ -linear functor. From theorem 6.3.6 it follows that $\mathcal{F}$ is bijective on isomorphism classes of objects. The map $Hom(M_1, M_2) \rightarrow Hom(\mathcal{F}(M_1), \mathcal{F}(M_2))$ is injective. By counting the dimensions of the two vectorspaces over $\mathbf{C}(z^m)$ one finds that the map is bijective.

We can describe the functor $\mathcal{F}$ in another more convenient way. Namely $\mathcal{F}M = M \otimes_{\mathbf{C}(z^m)} \mathbf{C}(z)e$ with the obvious structure as $Z[z]$ -module. $\mathcal{F}M$ has finite dimension over K . Therefore $\mathcal{F}M$ is also a $\hat{Z}[z]$ -module. The structure as left $\hat{\mathcal{D}}$ -module is defined by $\Phi(m \otimes fe) = cm \otimes f(qz)e$. We will consider this module as a left $\mathcal{D}$ -module of finite dimension over $\mathbf{C}(z)$. For two Z -modules M_1, M_2 of finite dimension one defines a $\mathbf{C}(z)$ -linear isomorphism

$$\begin{aligned} (\mathcal{F}M_1) \otimes (\mathcal{F}M_2) &= (M_1 \otimes_{\mathbf{C}(z^m)} \mathbf{C}(z)e) \otimes (M_2 \otimes_{\mathbf{C}(z^m)} \mathbf{C}(z)e) \rightarrow \\ &= (M_1 \otimes_{\mathbf{C}(z^m)} M_2) \otimes_{\mathbf{C}(z^m)} \mathbf{C}(z)e = \mathcal{F}(M_1 \otimes_{\mathbf{C}(z^m)} M_2) \end{aligned}$$

by

$$(m_1 \otimes f_1 e) \otimes (m_2 \otimes f_2 e) \rightarrow (m_1 \otimes m_2) \otimes f_1 f_2 e.$$

Obviously this is an isomorphism of left $\mathcal{D}$ -modules of finite dimension over $\mathbf{C}(z)$.
 $\square$

Definition 6.3.8 *The m -curvature of a $\mathcal{D}$ -module over $\mathbf{C}(z)$ is the $\mathbf{C}(z^m)$ -linear map Φ^m on the module N with $\mathcal{F}(N) = M$. We will call the $\mathbf{C}(z)$ -linear map Φ^m on $M = N \otimes_{\mathbf{C}(z^m)} \mathbf{C}(z)$ also the m -curvature.*

Consider the system of q -difference equations $\phi(\mathbf{y}) = A\mathbf{y}$, where $A \in Gl(n, \mathbf{C}(z))$. Let M be the q -difference module associated to this system of q -difference equations. Then the m -curvature as a $\mathbf{C}(z)$ -linear map on M has the matrix $A^{-1}(q^{m-1}z) \cdots A^{-1}(qz)A^{-1}(z)$.

6.4 Tannakian Categories and the q -Difference Galois Group

In the previous section we have shown that the category $Dif f_{\mathbf{C}(z)}$ of left $\mathcal{D}$ -modules of finite dimension over $\mathbf{C}(z)$ and the category $FMod_Z$ of Z -modules of finite dimension over $\mathbf{C}(z^m)$ are equivalent. First we will take a closer look at the category $FMod_Z$.

Now let L be any field. We want to describe the category $FMod_{L[t, t^{-1}]}$ of all $L[t, t^{-1}]$ -modules of finite dimension over L in more detail. A module is a finite dimensional vector space M over L together with an invertible linear map t . For the terminology of Tannakian categories we refer to [DM82]. The tensor product is already defined in the previous section. The identity object $\mathbf{1}$ is the one dimensional module Le together with the invertible L -linear map t which is given by $te = e$. The internal Hom is given as $\underline{Hom}(M, N) = Hom_L(M, N)$ with the $L[t, t^{-1}]$ -structure given by $(tl)(m) = t^{-1}(l(tm))$ for $l \in Hom_L(M, N)$ and $m \in M$. The category $FMod_{L[t, t^{-1}]}$ is a rigid, abelian, L -linear tensor category. Let $Vect_L$ denote the category of finite dimensional vector spaces over L and let $\omega : FMod_{L[t, t^{-1}]} \rightarrow Vect_L$ be the forgetful functor given by $\omega(M) = M$. That is one forgets the action of t on M . One can verify that ω is a fibre functor. Hence $FMod_{L[t, t^{-1}]}$ is a neutral Tannakian category over L . Associated to this neutral Tannakian category there is an affine group scheme over L , which represents the functor $R \mapsto Aut^{\otimes}(\omega)(R)$ defined on L -algebras.

For an object $M \in FMod_{L[t, t^{-1}]}$ one can consider the full subcategory $\{\{M\}\}$ of $FMod_{L[t, t^{-1}]}$ generated by M . The objects of this category are the subquotients of the tensor products $M \otimes \cdots \otimes M \otimes M^* \otimes \cdots \otimes M^*$, where M^* denotes the dual of M . The restriction of ω to $\{\{M\}\}$ is again a fibre functor. The affine linear group associated to this $\{\{M\}\}$ is denoted by G_M . In fact G_M is the smallest linear algebraic subgroup of $Gl(M)$, which contains the action of t on M . If

$\text{char}(L) = 0$ and L is algebraically closed then G_M is a direct product of a torus, a finite cyclic group and if t is not semisimple a $\mathbf{G}_{a,L}$.

Now let M be $\mathcal{D}$ -module over $\mathbf{C}(z)$ and let N be the Z -module with $\mathcal{F}(N) = M$. Let $\{\{M\}\}$ denote the full subcategory of $\text{Diff}_{\mathbf{C}(z)}$ generated by M then the functor $\mathcal{F} : F\text{Mod}_Z \rightarrow \text{Diff}_{\mathbf{C}(z)}$ induces an equivalence $\{\{N\}\} \rightarrow \{\{M\}\}$ of tensor categories. Hence $\{\{M\}\}$ is also a neutral Tannakian category. Its fibre functor is $\omega \circ \mathcal{F}^{-1} : \{\{M\}\} \rightarrow \text{Vect}_{\mathbf{C}(z^m)}$.

Definition 6.4.1 *The difference Galois group G of M is the linear algebraic group over $\mathbf{C}(z^m)$ associated to this fibre functor.*

If $\mathcal{F}(N) = M$ then the difference Galois group G of M is isomorphic to the group G_N as defined above. Hence the difference Galois group G associated to a system of difference equations is the linear algebraic group generated by the m -curvature.

Example. Consider the first order equation $\phi(y) = ay$, where $a \in \mathbf{C}(z)$. Then the m -curvature is equal to $\tilde{a} = \frac{1}{a(q^{m-1}z) \cdots a(qz)a(z)}$. Hence the difference Galois group associated to this first order difference equation is finite cyclic of order k if and only if $\tilde{a}$ is a primitive k th root of unity. Otherwise if $\tilde{a}$ is not a root of unity then the difference Galois group is the group $\mathbf{G}_{m,\mathbf{C}(z^m)}$ i.e. the multiplicative group over the field $\mathbf{C}(z^m)$.

Example. Consider the hypergeometric q -difference equation which is given by

$$\phi^2(y) + \frac{(-4 + q^\alpha + q^\beta)z + 3 - q^{\gamma-1}}{z-1}\phi(y) + \frac{(2 - q^\alpha)(2 - q^\beta)z - 2 + q^{\gamma-1}}{z-1}y = 0.$$

We are interested in the case where α, β and γ are integral parameters and q is a root of unity. As usual we will identify the second order q -difference equation with the system (A) : $\phi \mathbf{y} = \begin{pmatrix} 0 & 1 \\ -b & -a \end{pmatrix} \mathbf{y}$, where $a = \frac{(-4+q^\alpha+q^\beta)z+3-q^{\gamma-1}}{z-1}$ and $b = \frac{(2-q^\alpha)(2-q^\beta)z-2+q^{\gamma-1}}{z-1}$. Note that the hypergeometric equation is symmetric in the parameters α and β . This restricts the number of possibilities we have to consider.

If $q = 1$ then the system of q -difference equations (A) simplifies to $\phi \mathbf{y} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \mathbf{y}$. The 1-curvature has the matrix $A^{-1} = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$. Hence the 1-curvature has two eigenvalues 1 but is not semisimple. Therefore the q -difference Galois group G is isomorphic to the additive group $\mathbf{G}_a(\mathbf{C}(z)) = \{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbf{C}(z) \}$.

If $q = -1$ then the 2-curvature has the matrix $A(-z)^{-1}A(z)^{-1}$. We distinguish six cases.

1. If $\alpha \equiv 0 \pmod{2}$, $\beta \equiv 0 \pmod{2}$ and $\gamma \equiv 0 \pmod{2}$ then the 2-curvature has eigenvalues 1 and $\frac{z^2-1}{z^2-9}$. The q -difference Galois group G is isomorphic to the group $\{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \mid d \in \mathbf{C}(z^2)^* \}$.
2. If $\alpha \equiv 1 \pmod{2}$, $\beta \equiv 0 \pmod{2}$ and $\gamma \equiv 0 \pmod{2}$ or $\alpha \equiv 0 \pmod{2}$, $\beta \equiv 1 \pmod{2}$ and $\gamma \equiv 0 \pmod{2}$ then the 2-curvature has eigenvalues 1 and $\frac{1}{9}$. The q -difference Galois group G is isomorphic to the group $\{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \mid d \in \mathbf{C}(z^2)^* \}$.
3. If $\alpha \equiv 1 \pmod{2}$, $\beta \equiv 1 \pmod{2}$ and $\gamma \equiv 0 \pmod{2}$ then the 2-curvature has eigenvalues $\frac{1}{9}$ and $\frac{z^2-1}{9z^2-1}$. The q -difference Galois group G is isomorphic to the group $\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbf{C}(z^2)^* \}$.
4. If $\alpha \equiv 0 \pmod{2}$, $\beta \equiv 0 \pmod{2}$ and $\gamma \equiv 1$ then the 2-curvature has matrix $\begin{pmatrix} 3 & -2 \\ 2 & -1 \end{pmatrix}$. Hence both eigenvalues of the 2-curvature are equal to 1 but the 2-curvature is not semisimple. The q -difference Galois group G is isomorphic to the additive group $\mathbf{G}_a = \{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbf{C}(z^2) \}$.
5. If $\alpha \equiv 1 \pmod{2}$, $\beta \equiv 0 \pmod{2}$ and $\gamma \equiv 1 \pmod{2}$ or $\alpha \equiv 0 \pmod{2}$, $\beta \equiv 1 \pmod{2}$ and $\gamma \equiv 1 \pmod{2}$ then the 2-curvature has eigenvalues 1 and $\frac{z^2-1}{9z^2-1}$. The q -difference Galois group G is isomorphic to the group $\{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \mid d \in \mathbf{C}(z^2)^* \}$.
6. If $\alpha \equiv 1 \pmod{2}$, $\beta \equiv 1 \pmod{2}$ and $\gamma \equiv 1 \pmod{2}$ then the 2-curvature has eigenvalues $\frac{z-1}{9z-1}$ and $\frac{z+1}{9z+1}$. Note that also in this case the set of eigenvalues is invariant under the map $z \mapsto -z$. The q -difference Galois group G is a non-split two dimensional torus which is isomorphic to two copies of the multiplicative group $\mathbf{G}_m$ after the field extension $\mathbf{C}(z) \supset \mathbf{C}(z^2)$.

Bibliography

- [Bat67] P.M. Batchelder, An introduction to linear difference equations, Dover Publications, New York (1967).
- [BBH88] F. Beukers, W.D. Brownawell, G. Heckman, Siegel normality, *Ann. of Math.* 127 (1988), 279 - 308.
- [BD79] Baldassarri, F. and Dwork, B. Differential equations with algebraic solutions. *American Journal of Mathematics* **101**(1) (1979)., 42–76.
- [Ber90] D. Bertrand, Extensions de D -modules et groupes de Galois différentiels, p -adic analysis, Lecture Notes in Mathematics 1454, Springer-Verlag, Berlin, Heidelberg, New York 1990.
- [Bli17] Blichfeldt, H.F. *Finite collineation groups*. Chicago: University of Chicago Press 1917.
- [Bro92] Bronstein, M. Linear ordinary differential equations; breaking through the order 2 barrier. *Proceedings of ISSAC 1992*. Berkeley: ACM Press.
- [DM82] P. Deligne, J. Milne, Tannakian categories, *Lect. Notes in Math.* **900**, 101-228, 1982.
- [Gre69] M.J. Greenberg, Lectures on forms in many variables, W.A. Benjamin, Inc., New York, 1969.
- [Hen96] P.A. Hendriks, An algorithm for determining the difference Galois group for second order linear difference equations, To appear in *J. Symb. Comp.*
- [HP93] Hendriks, P. A., van der Put, M. A rationality result for Kovacic's algorithm. *Proceedings of ISSAC 1993*. Berkeley: ACM Press.
- [HP95] P.A. Hendriks, M. van der Put, Galois action on solutions of differential equations, *J. Symb. Comp.* 19 (1995), 559-576
- [Kap57] I. Kaplansky, An introduction to differential algebra, Hermann, Paris, 1957.

- [Kol68] E.R. Kolchin, Algebraic groups and algebraic independence, Amer. J. Math. 90 (1968), 1151-1164.
- [Kol73] E.R. Kolchin, Differential algebra and algebraic groups, Academic Press, New York, London, 1973.
- [Kov86] J.J. Kovacic, An algorithm for solving second order linear differential equations, J. Symb. Comp. 2 (1986), 3-43.
- [Lev75] Levelt, A.H.M. Jordan decomposition for a class of singular differential operators. *Arkiv för matematik*, **12**(1) (1975), 1-27.
- [Lev90] A.H.M. Levelt, Differential Galois theory and tensor products, Indag. Math. 1 No. 4 (1990), 439-449.
- [Pet92] M. Petkovsek, Hypergeometric solutions of linear recurrences with polynomial coefficients, J. Symb Comp. 14 (1992), 243-264.
- [PS96] M. van der Put, M.F. Singer, Galois theory of difference equations, in preparation.
- [Put95] M. van der Put, Differential equations in characteristic p , *Compositio mathematica* **97** (1995), 227-251
- [Ren75] G. Renault, *Algebre non commutative*, Gautiers-Villars, Paris, 1975.
- [Ser64] J-P.Serre, *Cohomologie Galoisienne*, Lecture Notes in Mathematics, Springer-Verlag, New York, 1964.
- [Ser68] J-P.Serre, *Corps locaux*, Hermann, Paris, 1968.
- [Shi89] A.B. Shidlovskii, *Transcendental numbers*, de Gruyter Studies in Mathematics 12, Walter de Gruyter, Berlin, New York, 1989.
- [Sin89] M.F. Singer, An outline of differential Galois theory, *Computer Algebra and Differential Equations*, E. Tournier (editor), Academic Press, 1990.
- [SU93] Singer, M.F. and Ulmer, F. Liouvillian and algebraic solutions of second and third order linear differential equations. *Journal of Symbolic Computation* **16**(1) (1993), 9-13.

Samenvatting

Dit proefschrift behandelt enkele algebraïsche en algoritmische aspecten van differentiaal-, differentie- en q -differentievergelijkingen.

Het grootste gedeelte van dit proefschrift gaat over algoritmes die nagaan of een gegeven tweede orde differentiaal-, differentie- of q -differentievergelijking *elementaire oplossingen* heeft en als eventueel resultaat deze oplossingen bepaalt. Dit noemt men het symbolisch oplossen van vergelijkingen. Het begrip *elementaire oplossing* is hierbij zeer precies gedefinieerd.

Voor tweede orde lineaire differentiaalvergelijkingen heeft Kovacic in 1986 als eerste een algoritme ontwikkeld. Dit algoritme is gebaseerd op de Galoistheorie van differentiaalvergelijkingen. Er zijn versies van dit algoritme geïmplementeerd in de computeralgebra pakketten Maple en Mathematica. Het algoritme van Kovacic was verre van volmaakt omdat dit algoritme op een chaotische manier algebraïsche getallen introduceerde. Daardoor werkte het algoritme in de praktijk in sommige gevallen slecht of helemaal niet. In hoofdstuk 2 van dit proefschrift wordt theorie beschreven die voorspelt welke algebraïsche uitbreidingen van het getallenlichaam echt nodig zijn om tweede en derde orde differentiaalvergelijkingen symbolisch op te lossen. Deze theoretische resultaten helpen om het algoritme van Kovacic te verbeteren.

Recentelijk hebben M. van der Put en M.F. Singer Galoistheorie voor differentievergelijkingen ontwikkeld. De algoritmes voor het symbolisch oplossen van tweede orde differentie- en q -differentievergelijkingen die worden gepresenteerd in respectievelijk hoofdstuk 4 en 5 van dit proefschrift zijn op deze theorie gebaseerd. Deze algoritmes kunnen worden beschouwd als het analogon voor differentie- en q -differentievergelijkingen van Kovacic's algoritme voor differentiaalvergelijkingen. De *elementaire oplossingen* waarnaar gezocht wordt liggen in het geval van differentie en q -differentievergelijkingen in een zekere rijtjesruimte.

Siegel-normaliteit en Shidlovskii-irreducibiliteit zijn begrippen die een belangrijke rol spelen in een tak van de transcendente getaltheorie. Als een systeem van lineaire differentiaalvergelijkingen Siegel-normaal of Shidlovskii-irreducibel is, dan zegt dat iets over de algebraïsche (on)afhankelijkheid van de oplossingen van het systeem van differentiaalvergelijkingen. De Galoistheorie van differentiaalvergelijkingen gaat ook over algebraïsche relaties tussen de oplossingen van een differentiaalvergelijking. In Hoofdstuk 3 van dit proefschrift wordt dit met elkaar in verband gebracht.

In Hoofdstuk 6 van dit proefschrift worden de q -differentievergelijkingen geclassificeerd, waarbij q een eenheidswortel is. Als q een eenheidswortel is, dan is de Galoistheorie voor differentievergelijkingen, zoals die is ontwikkeld door M. van der Put en M.F. Singer niet geheel bevredigend. Dit is te wijten aan het feit dat

het constantenlichaam in dit geval niet algebraïsch gesloten is. Het blijkt bijvoorbeeld niet mogelijk te zijn om de q -differentie Galoisgroep voor deze vergelijkingen op de gebruikelijke wijze te definiëren. Met behulp van de theorie van Tannaka categorieën wordt dit probleem omzeild en blijkt het wel mogelijk te zijn om de q -differentie Galoisgroep op een geschikte manier te definiëren.

Nawoord

Aan het eind van dit boekje wil ik nog een aantal mensen bedanken.

Verreweg de meeste dank ben ik verschuldigd aan Marius van der Put. Zijn ideeën, zijn enthousiasme en zijn prettige wijze van begeleiden hebben mij steeds enorm gestimuleerd.

Frits Beukers wil ik bedanken voor zijn bijdrage aan het hoofdstuk over Shidlovskii-irreducibiliteit.

De leescommissie bestaande uit W. Dale Brownawell, Arjeh M. Cohen en Michael F. Singer bedank ik voor het doorlezen van het manuscript en voor hun commentaar.

Tenslotte wil ik mijn collega's bedanken, omdat zij mijn AIO/OIO-tijd tot een onvergetelijke hebben gemaakt. Het was erg vaak erg gezellig. In het bijzonder wil ik mijn kamergenoten Bert Kroese, Bernard Faber en Rene Jofriet noemen.